MARINHA DO BRASIL

ESCOLA DE GUERRA NAVAL

SUPERINTENDÊNCIA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS MARÍTIMOS

ALICE ALVES CASANOVA

NETWORKS AND PORTS: HOW THE CONCEPT OF SECURITY NETWORK CAN FOSTER INTERAGENCY COOPERATION IN BRAZILIAN PORT SECURITY

RIO DE JANEIRO

2022

ALICE ALVES CASANOVA

NETWORKS AND PORTS: HOW THE CONCEPT OF SECURITY NETWORK CAN FOSTER INTERAGENCY COOPERATION IN BRAZILIAN PORT SECURITY

Relatório Técnico (Policy Report) apresentado como requisito à obtenção do grau de Mestre em Estudos Marítimos ao Programa de Pós-Graduação em Estudos Marítimos (PPGEM) da Escola de Guerra Naval (EGN), na área de concentração Defesa, Governança e Segurança Marítimas.

Linha de Pesquisa: Regulação do Uso do Mar, Processo Decisório e Métodos Prospectivos (LP2).

Orientador: Prof. Dr. Thauan dos Santos

Coorientador: CMG (Refº) Claudio Rogério de Andrade Flôr

RIO DE JANEIRO

2022

C334n Casanova, Alice

Networks and ports: how the concept of security network can foster interagency cooperation in brazilian port security / Alice Casanova. - Rio de Janeiro, 2021.

97 f. : il.

Dissertação (Mestrado) - Escola de Guerra Naval, Programa de Pós-Graduação em Estudos Marítimos (PPGEM), 2021.

Orientador: Thauan dos Santos

Coorientador: Claudio Rogério de Andrade Flôr

Bibliografia: f. 91-97

1. Cooperação interagências. 2. Proteção portuária. 3. Redes criminosas. I. Redes de segurança. II. Escola de Guerra Naval. (Brasil). II. Título.

CDD 387.1

Ficha catalográfica elaborada pela bibliotecária
Cremilda Santos – CRB7/3200
Biblioteca da Escola de Guerra Naval

ALICE ALVES CASANOVA

NETWORKS AND PORTS: HOW THE CONCEPT OF SECURITY NETWORK CAN FOSTER INTERAGENCY COOPERATION IN BRAZILIAN PORT SECURITY

Relatório Técnico (Policy Report) apresentado como requisito à obtenção do grau de Mestre em Estudos Marítimos ao Programa de Pós-Graduação em Estudos Marítimos (PPGEM) da Escola de Guerra Naval (EGN), na área de concentração Defesa, Governança e Segurança Marítimas.

Aprovada em 22 de julho de 2022.

Banca Examinadora:

_____

Dr. Thauan dos Santos
Professor Doutor, Escola de Guerra Naval

_____

CMG (Refº) Claudio Rogério de Andrade Flôr
Professor Mestre

_____

CMG (RM1-FN) Dr. Adriano Lauro
Professor Doutor, Escola de Guerra Naval

_____

Dra. Daniele Dionísio da Silva
Professora Doutora, Universidade Federal do Rio de Janeiro

ABSTRACT

Ports are vital infrastructures accounting for 90% of the global trade by concentrating a vast flow of goods, assets, and people. Transnational Organized Crime (TOC), operating in the form of networks, uses maritime routes and port facilities to carry out a range of illicit activities, including drugs and weapons trafficking, smuggling of counterfeit goods and other merchandise, and human trafficking. To tackle the complex and networked nature of organized crime, port security governance of some major international seaports has adopted different law enforcement approaches, from interagency arrangements such as joint task forces and security networks to hybrid policing. In Brazil, there has been in recent years a significant rise in cocaine seizures by law enforcement in the country's major ports, notably the Port of Santos, which shows that transnational criminal organizations are using Brazilian seaports are "gateways" to overseas cocaine markets. In this context, security practitioners in Brazil recognize the crucial role that interagency cooperation plays in tackling criminality in ports. This report intents to build awareness on transnational criminal organizations operating as Criminal Networks, and how the concept of Security Network is vital to disrupt the illicit activities of this type of criminality. The aim is to contribute to disseminate a "network perspective" among Brazilian public security policy and decision makers and security providers, as well as academia. For this, we take on a multidisciplinary approach, drawing from the methodologies and theories of Social Network Analysis (SNA), and the network perspective adopted in Public Management, Organizational studies, and in Criminology and Security studies. Finally, this report proposes an illustrative model of a Knowledge-Generating Security Network for the Port of Santos, which would foster information and knowledge sharing on organized crime threat assessment and disseminate security best practices to leverage interagency cooperation among port's security providers and other organizations.

Keywords: Port Security; Interagency Cooperation; Security Networks; Criminal Networks

RESUMO

Portos são infraestruturas vitais ao concentrar 90% do comércio global através do fluxo de mercadorias, ativos e pessoas. O Crime Organizado Transnacional (COT), atuando na forma de redes, tem utilizado as rotas marítimas e as instalações portuária para realizar uma série de crimes, que incluem tráfico de drogas, armas e pessoas, além de contrabando de mercadorias falsificadas. Para combater a natureza complexa e em redes do crime organizado, a governança da proteção portuária dos principais portos internacionais, especialmente nos EUA, União Europeia e Australia, tem adotado diferentes abordagens como arranjos interagências através de forças-tarefa conjuntas e redes de segurança e também o policiamento híbrido. No Brasil, nos últimos anos, houve um crescimento significante do número de apreensões de toneladas de cocaína nos principais portos de exportação do país, em especial no Porto de Santos. Isso demonstra que o crime organizado transnacional tem utilizado de forma recorrente os portos brasileiros como "portões" para escoar a produção da cocaína produzida nos países andinos para o mercado consumidor estrangeiro, principalmente o europeu. Neste contexto, os agentes de proteção portuária do país reconhecem a importância da cooperação interagências no combate aos crimes cometidos nos portos. Este relatório visa conscientizar o leitor sobre o crime organizado transnacional atuando na forma de Redes Criminosas (*Criminal Networks*) e como o conceito de Redes de Segurança (*Security Networks*) é crucial para se combater as atividades ilícitas deste tipo de criminalidade. O objetivo é disseminar uma "perspectiva de redes" (*network perspective*) entre tomadores de decisão, agentes de segurança pública e também no meio acadêmico. Para tanto, aplicamos uma abordagem multidisciplinar, utilizando a metodologia de Análise de Redes Sociais (*Social Network Analysis*), além da perspectiva de redes descrita nas literaturas internacionais de Administração Pública, Estudos Organizacionais e Estudos de Segurança e Criminalidade. Por fim, o relatório propõe um modelo ilustrativo de uma Rede de Segurança para Geração de Conhecimento voltada para a proteção do Porto de Santos. A rede tem como objetivo promover a troca de informação e conhecimento acerca da avaliação de ameaças do crime organizado e ainda disseminar boas práticas de segurança pública, com a intenção de aprimorar a cooperação interagências entre os agentes de proteção portuária e outras organizações.

Palavras-chave: Proteção Portuária; Cooperação Interagências; Redes de Segurança; Redes Criminosas

Executive Summary

Ports are vital infrastructures accounting for 90% of the global trade by concentrating a vast flow of goods, assets, and people. Transnational Organized Crime (TOC), operating in the form of networks, uses maritime routes and port facilities to carry out a range of illicit activities, including drugs and weapons trafficking, smuggling of counterfeit goods and other assets, and human trafficking. To tackle the complex and networked nature of organized crime, port security governance of some major international seaports has adopted different law enforcement approaches, from interagency arrangements, such as joint task forces and security networks, to hybrid policing.

Brazil is nowadays considered the main transit route for cocaine trafficking to Europe, Africa, and Asia. There has been in recent years a significant rise in cocaine seizures by law enforcement in the country's major ports, notably the Port of Santos, which shows that transnational criminal organizations are using Brazilian seaports are "gateways" to overseas cocaine markets. Security practitioners in Brazil recognize the crucial role that interagency cooperation plays in tackling criminality in ports. However, interagency cooperation in the country faces challenges and limitations in relation to conflicting mandates and jurisdiction of agencies, duplication or dispersion of efforts, lack of integration among actors, shortage of resources and personnel to carry out operations, limiting budgets and capacity, and time-consuming planning.

In the context of the criminality carried out in ports and the need to foster interagency cooperation among port security providers, this report intents to build awareness on transnational criminal organizations operating as Criminal Networks, and how the concept of Security Network is vital to disrupt the illicit activities of such "dark" networks. The aim is to contribute to disseminate a "network perspective" among Brazilian public security police and decision makers and security providers, as well as academia. For this, we take on a multidisciplinary approach, drawing from the methodologies and theories of Social Network Analysis (SNA), and the network perspective adopted in Public Management, Organizational studies, and in Criminology and Security studies. Finally, this report proposes an illustrative model of a Knowledge-Generating Security Network for the Port of Santos, which would promote information and knowledge sharing on organized crime threat assessment and disseminate security best practices to leverage interagency cooperation among port's security providers and other organizations.

Key topics in this report include:

- Interagency Cooperation arises from the need for public agencies and stakeholders to span boundaries and work across sectors to address a myriad of complex and challenging issues that call for the resources and expertise of different agencies.

- Inter-organizational networks, as a governance form, provide adaptability and flexibility in contrast to hierarchy and market types. Networks are a suitable choice in dealing with "wicked" problems, such as terrorism and transnational organized crime, which require collective action, that is, a group of three or more actors working towards a common goal.

- Criminal networks, or "dark networks", are loose associations of criminals, without a clear center of gravity, cooperating to achieve a profit-driven goal. In today's globalized environment, they are considerate more efficient than hierarches such as the traditional Italian mafia groups. Criminal networks are known for their transnational, decentralized, and adaptable nature, making them resilient to law enforcement disruption efforts. The versatility of networks allows them to change operations rapidly and to quickly exploit new opportunities.

- The concept of Security Networks refers to a set of actors that are directly or indirectly connected in order to authorize and/or deliver security for the benefit of internal or external stakeholders. As interagency arrangements, they promote cooperation by means of mobilization of resources and capacity, as well sharing of information, knowledge, and intelligence.

- Criminality in international and Brazilian seaports entails complex crimes carried out by transnational criminal networks. Cocaine trafficking is the main security concern in Brazilian ports. Criminals are very creative in hiding drugs in regular cargos, containers, and inside ship's compartments to dodge surveillance and control checks. They also practice corruption of port operators and personnel to obtain information on port logistics and supply chain.

- International port security governance involves different law enforcement approaches such as interagency arrangements, in the form of joint task forces and security networks, and hybrid policing. Challenges include cooperation and coordination problems regarding agencies' jurisdiction, mandates, overlapping legal attributions, conflicting priorities, mentalities, and agencies with different and sometimes divergent organizational cultures.

- In Brazil, port security relies on *ad hoc* interagency operations to counter drug trafficking. Most cocaine seizures and drug traffickers' arrests in ports and vessels usually happen under coordinated efforts between a number of security actors, such as NEPOM (the Federal Maritime Police), the Federal Revenue Office, Port Authority Guard, the Brazilian Navy, and other regulatory agencies.

- To attain more stronger integration among security agencies to tackle criminal networks, security practitioners in Brazil argue for the need to create new policies, strategies, and joint commands. In this context, interagency cooperation could benefit from flexibility and adaptability by adopting a network perspective on security. The concept of Security Network seems one optimal arrangement to achieve more sustainable and resilient cooperation and coordination among Brazilian agencies.

- The Knowledge-Generating Security Network for the Port of Santos proposed by this report intends to educate security providers on the potentialities of the network approach to security. The network would support knowledge and information sharing on organized crime threat assessment, disseminate security best practices, and foster advanced learning, strengthening the synergy amid public and private security actors within the security governance of the Port of Santos. The main outcome of the network would be to support a more substantiable and long-term interagency cooperation among the security providers of the port.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABREVIATIONS

ABIN - Agência Brasileira de Inteligencia [Brazilian Intelligence Agency]
ANTAQ - Agência Nacional de Transportes Aquaviários [National Waterway Transport Agency]
CV - Comando Vermelho [Red Command]
CESPORTOS - Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis [State Commissions for Public Security of Ports, Terminals, and Waterways]
CONPORTOS - Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis [National Commission for Public Security of Ports, Terminals and Waterways]
CCP - Container Control Programme
FA - Forças Armadas [Armed Forces]
GSI/PPIF - Gabinete de Segurança Institucional/Programa de Proteção Integrado de Fronteiras [Institutional Security Office of the Federal Government/The Integrated Program for Border Protection]
IMO - International Maritime Organization
ISPS - International Ship and Port Facility Security Code
MB – Marinha do Brasil [Brazilian Navy]
MD – Ministério da Defesa (Ministry of Defense]
ME – Ministério da Economia [Ministry of Economy]
MI – Ministério da Infraestrutura (Ministry of Infrastructure]
MJSP – Ministério da Justiça e Segurança Pública [Ministry of Justice and Public Security]
MRE – Ministério das Relações Exteriores [Ministry of Foreign Affairs]
NAO - Network Administrative Organization
NEPOM - Núcleo Especial de Polícia Marítima [Federal Maritime Police]
OECD - Organization for Economic Co-operation and Development
PCC - Primeiro Comando da Capital [First Command of the Capital]
PF - Policia Federal [Federal Police]
PFSO - Port Facility Security Officers
PRF - Polícia Rodoviária Federal [Federal Highway Police]
PSKN - Public Sector Knowledge Network
RFB - Receita Federal do Brasil [Federal Revenue Office]
SEOIP - Secretaria de Operações Integradas - Ministério da Justiça e Segurança Pública [Integrated Operations Office - Ministry of Justice and Public Security]
SPA - Santos Port Authority
SNA - Social Network Analysis
SOLAS - The International Convention for the Safety of Life at Sea
SWT - Strength of Weak Ties
TCU - Tribunal de Contas da União [Brazilian Federal Court of Accounts]
TOC - Transnational Organized Crime
UNODC - United Nations Office on Drugs and Crime
UNTOC - UN Convention against Transnational Organized Crime

TABLE OF CONTENTS

Introduction

With 90% of all global trade carried out by sea via container ships and other trade vessels, seaports are important logistics spaces and hubs for maritime transportation and supply chain (OECD, 2019). As central nodes in the globalization network, these infrastructures concentrate a constant flow of goods, assets, and people. Ports not only play a crucial role in the global economy, but they also play a strategic role in the illicit market, in special the activities of Transnational Organized Crime (TOC). Criminals use ports as "doors" to the land and "gateways" to the sea (SERGI, 2020a) to carry out a spectrum of illicit activities, from drug and arms trafficking, smuggling of counterfeit goods and other assets, human trafficking, to corruption and infiltration in the legal economy of ports. Besides, transnational criminal organizations operate as highly adaptable and flexible criminal networks, which are resilient to law enforcement disruption efforts.

In the case of Brazil, with its vast maritime frontier, seaports are vital infrastructure for the country's supply chain and economy. The increasing number of drug seizures over the last years in the main exporting ports in Brazil, notably in the Port of Santos and the Port of Paranaguá, shows that criminal organizations are using port spaces and logistics to export huge amounts of cocaine to consumer markets in Europe, Africa, and Asia. Drug trafficking is considered the main threat to port security in Brazil, with the potential to cause disruption in port operations. The prevention and repression of drug tracking is today the main concern of public authorities and port security providers in the country.

Port security governance takes place in a multiplex environment with a myriad of public and private actors performing different tasks, mandates, and legal responsibilities, such as regulatory, customs, law enforcement, and private security companies. Furthermore, given the complex and transnational nature of drug trafficking organizations and their networked *modus operandi*, the provision of security in ports requires collective action in the form of interagency cooperation. As a process, interagency cooperation entails different public and private actors to span across sectors to work towards a common goal. This type of cooperation is multifaced and involves differing organizational structures, legal authorities, duties, and resource and capacity levels, which sometimes may diverge or overlap, hampering interaction among agencies (STRICKLER, 2010).

In Brazil, security practitioners highlight the crucial role that interagency cooperation, such as joint task forces, play in tackling criminality in ports. Most cocaine seizures and drug traffickers' arrests in ports and vessels usually happen under coordinated efforts between a

number of security actors, such as NEPOM (The Federal Maritime Police), the Federal Revenue Office, the Brazilian Navy, and other regulatory agencies, for instance. The cooperation with the Port Authority Guard and private security organizations is also important for the effectiveness of such operations in port facilities. Interagency cooperation faces challenges and limitations in the Brazilian context in relation to conflicting mandates and jurisdictions of agencies, duplication or dispersion of efforts, lack of integration among agencies and shortage of resources and personnel to carry out operations, limiting budgets, and time-consuming planning. Difficulties in the provision of port security, according to the Brazilian Federal Court of Accounts (TCU, 2021), include NEPOM's lack personnel and resources (such as patrol vessels) to carry out their work efficiently. Some port facilities were found to not fully adhere to CONPORTOS security provisions in relation to the ISPS Code. Moreover, CONPORTOS/CESPORTOS sometimes have difficulty in integrating security providers in some port environments.

Research on criminality in major international ports show that criminal networks may take advantage of bottlenecks, vulnerabilities, and relational conflicts in this interagency environment to exploit opportunities to carry out their illicit activities, while also potentially influencing and coopting port operators. Therefore, the provision of port security is a complex task that requires a better understanding of port flows and networks (SERGI, 2020b).

In the context of the criminality and the multifaceted security arrangements of ports, this report intents to build awareness on transnational criminal organizations operating as Criminal Networks and how the concept of Security Network is vital to disrupt the illicit activities of such "dark" networks. The aim is to contribute to disseminate a "network perspective" among public security policy and decision makers and security providers, as well as academia. For this, we take on a multidisciplinary approach, drawing from the methodologies and theories of Social Network Analysis (SNA) used to map, measure, and analyze the social structure and relationships between individuals, groups, and organizations. The report also employs the network perspective adopted in Public Management and Organizational studies and in Criminology and Security studies to conduct the discussions on Criminal Networks, the concept of Security Network, and port criminality and security governance.

In Security studies, a network is viewed as a type of governance form, in the sense that the public administration of security takes place with and through networks (WHELAN, 2012). To better understand the concept of Security Network, this report draws on the Public Management and Organizational literatures, which describe Inter-Organizational Networks "as a group of three or more autonomous organizations connected in ways that facilitate the

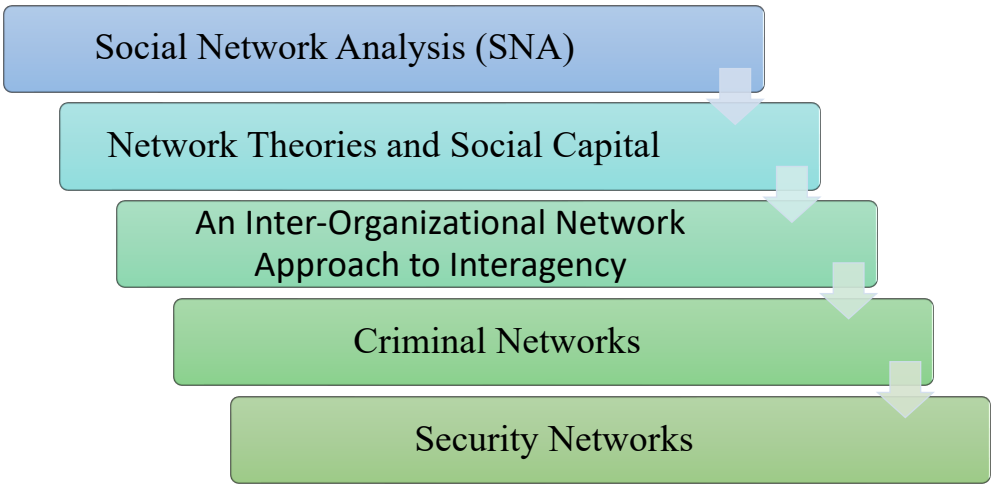
achievement of a common goal" (PROVAN; SYDOW, 2007, p. 482). In this light, the concept of Security Network refers to a set of institutional, organizational, or individual actors that are directly or indirectly connected in order to authorize and/or deliver security for the benefit of internal or external stakeholders. These actors are interconnected through different relational ties on a voluntary, contractual, or regulatory basis (DUPONT, 2006). As interagency arrangements, security networks promote cooperation by means of mobilization of resources and capacity, as well sharing of information, knowledge, and intelligence.

This report is divided in two overarching chapters and was developed having in mind readers with no previous knowledge on the network perspective. The first chapter begins by presenting an overview of SNA and its key theoretical approaches of Structural Hole (BURT, 1995, 2001, 2004) and Closure (COLEMAN, 1988), together with the concept of Social Capital. Next, we present the characteristics of Inter-Organizational Networks (PROVEN; KENIS, 2008; MILWARD; PROVAN, 2006; PROVEN; LEMAIRE, 2012; POPP et al., 2014; PROVAN; SYDOW, 2007), and then proceed to discuss the network perspective adopted in Criminology and Security studies (GERSPACHER; DUPONT, 2007; BRIGHT; WHELAN, 2020; BRIGHT; MALM, 2019; DUPONT, 2006; WHELAN, 2017, 2012; WHELAN; DUPONT, 2017) by describing the dynamics of Criminal Networks and the purposes and characteristics of Security Networks.

The second chapter is divided in two parts. The first part discusses criminal network activities in international ports, which sets the background for the discussion on security governance tendencies and challenges in major seaports. This first part relies on empirical research findings (SERGI et al., 2021; SERGI 2020a; 2020b; 2020c; ANTONELLI 2020; ROKS et al. 2020) on port criminality and security arrangements and practices carried out in international ports located in the EU, USA, and Australia. We highlight some empirical studies on port security networks (DINCHEL; EASTON, 2021; ESKI, 2016; BREWER, 2012) and the contribution of this concept in leveraging port security in the face of criminal networks. The second part of the chapter discusses organized crime and the governance of port security in Brazilian major ports. Data for this part was gathered from official government sources, two seminars on maritime and port security promoted by government agencies, academic empirical research on Brazilian ports, the Port of Santos webpage, and mainstream media webpages. Finally, this report proposes an illustrative model of a Knowledge-Generating Security Network for the Port of Santos, which would promote information and knowledge sharing on organized crime threat assessment and disseminate security best practices to leverage interagency cooperation among the port's security providers and other organizations.

Chapter 1 – The Network Perspective

Roadmap to chapter



1.1 Social Network Analysis (SNA)

Since society's early dawn, people have always interacted and formed relationships for various purposes. These social interactions can be depicted as networks between individuals, groups, or organizations (YANG et al., 2017). The term "network" has been loosely employed as a metaphor to describe a multitude of social arrangements and has gained broad recognition with the advent of the World Wide Web and social media. In the field of Social Network Analysis (SNA), however, the term network has a precise meaning: a network consists of a set of actors or entities (ex: individuals, groups, or organizations) connected (or not) by relational ties of a specific kind (ex: cooperation) (BORGATTI; HALGIN, 2011). The pattern of ties yields a particular network structure, in which each actor occupies a certain position. Most of the theoretical and methodological aspects and analysis of networks derive from network structure, actor position, and nature and quality of relations (BORGATTI; HALGIN, 2011).

The growing popularity of SNA in different disciplines, such as Sociology, Psychology, Public Administration, and Economics, for example, is due to society's awareness of the complexities and interconnectedness of social systems (PRELL, 2012). The underlying assumptions of SNA rest on the relational structure of networks and its consequences. It influences actor's perceptions, attitudes, beliefs, decisions, and actions, as well as whole network outcome such as its effectiveness. A network usually occurs in a particular space and time and is not a static structure, but a dynamic process continually changing through actor's interactions. Moreover, the relational structure provides pathways in the network for assisting (or constraining) some kind of flow between actors as they interact, such as flows of knowledge and flows of material resources (KNOKE; YANG, 2020).

Network architecture encompasses structural and relational properties. The structural properties define the sociometry of the social network, while the relational properties entail the quality of connections within the network (YANG et al., 2017). It is worth noting that a relation is not an attribute of an actor, but a dyadic property of both participants, as long as they maintain their association (KNOKE; YANG, 2020). These network properties can be visually represented as matrices and graphs, which are mathematical models of the network relational structure. On a graph, actors are represented as nodes or vertices, and ties are represented as lines called edges or arcs as shown in figure 1 below.

Networks can be of different types. A one-mode network is a type in which all entities are the same aggregate level (e.g., they are either individuals or organizations). A network can be bipartite, that is, two sets of nodes with different levels of aggregate (ex: individuals - one

set of nodes – have a tie with each organization – the other set of nodes). The relational data of the network can be directional, in which the tie between a pair of actors is directed from one actor to another, therefore, it has an origin and destination that cannot change, or the relation can be undirectional, in which the tie does not have a direction. A network can be binary, if it only captures the presence or absence of ties or valued if it distinguishes the strength of ties on an ordinal or continuous scale. Finally, relations can be of many types, such as cooperation, transactional, communications, instrumental, sentiment, authority/power relations, kinship, and others. (YANG et al., 2017; KNOKE; YANG, 2020; WASSERMAN; FAUST, 2009).

Table 1: Types of Networks

Types of Networks		
One-mode Bipartite	Directional Undirectional	Binary Valued

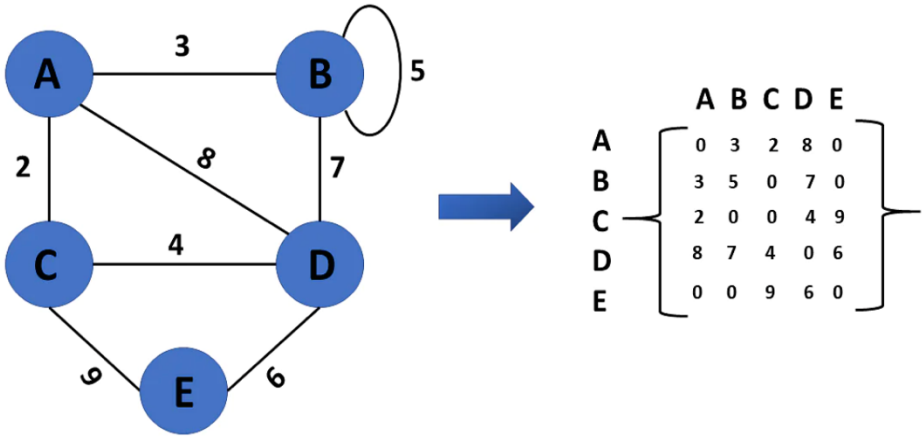


Figure 1: Examples of a graph (left) and a matrix (right) representations of a one-mode valued undirected network (SIMPLILEARN, 2022).

Regarding data collection, the research project's objective(s) is what defines the dataset, which entails selecting the set of actors (network boundary) and the type(s) of relations to be measured. Network data can be gathered through a variety of ways such as questionnaires, interviews, observations, archival records, experiments, and other techniques. (KNOKE; YANG, 2020).

SNA involves different analysis levels (units of observation) and measurements. The levels of analysis are: Actor (or Ego), Dyad (pairs of Egos), Triad (three actors connected in a

way that “friends of friends are likely to be friends”), Subgroups or Clusters (substructures in which actors are connected to each other in a particular way) or Whole Network (set of actors) (YANG et al., 2017; KNOKE; YANG, 2020). Usually, network research combines different level of analysis, allowing to connect micro-level behavior (e.g., Ego or Dyad) to macro-level environments (e.g., Whole Network). For each level of analysis, there are specific measurements, as seen in the table below:

Table 2: Network analysis levels and measures (adapted from KNOKE; YANG, 2020)

Analysis Levels	**Measures**
Actor (Ego)	Centrality – Degree centrality; Closeness centrality; Betweenness centrality
Dyad	Walk; Path; Distance; Reachability; Geodesic
Subgroups or Clusters	Transitivity; Cliques
Whole Network	Size; Density; Centralization

1.2 Network Theoretical Approaches and Social Capital

Network scholars make use of different theoretical approaches and concepts to analyze and test hypothesis on relational structures. In this section, we present the concept of Social Capital and the theoretical approaches of Structural Hole (BURT, 1995, 2001, 2004) and Closure (COLEMAN, 1988). A fundamental concept in network theoretical approaches, Social Capital can be understood as the contextual complement to Human Capital. Social Capital is conceptualized by scholars (BOURDIEU, 1986; COLEMAN, 1988; BURT, 2001; PUTMAN, 2000; LIN, 2005) as a set of resources embedded in relational ties that are advantageous for an actor in a social structure. A broader definition of the term also includes norms, trust, and values associated to social relations, which facilitate collective action.

To Burt (2001), Social Capital can be understood as metaphor about advantage, in the sense that an actor who do better is somehow better connected to others. “Certain people or certain groups are connected to certain others, trusting certain others, obliged to support certain others, dependent on the exchange with certain others” (BURT, 2001, p. 2). Social Capital is based on attributes of the relationships between actors, and it inheres in the relational structure of networks. Therefore, holding a certain position in the network can be asset and this asset is Social Capital. According to Burt’s theoretical approach, two network structures are argued to

create Social Capital: Closure and Structural Holes, these two models show how actors can be better connected (BURT, 2001).

The Structural Hole approach draws from Granovetter's theory on Strength of Weak Ties (SWT), which is based on two premises and its consequences. The first premise of SWT is that the stronger the tie between two people, the more likely their social worlds will overlap, and so they will probably have ties with the same third parties. The second premise states that a bridging tie is a potential source of new ideas and information, since it links a person to someone who is not connected to his/her friends. The strength of weak ties lies therefore in a bridge that connects two different close knits of close friends. In this view, actors with few weak ties will be deprived of novel information from distant parts of the social system, confining them to provincial information and viewpoints from their close friends. (GRANOVETTER,1973; BORGATTI; HALGIN, 2011).

Burt's approach entails that weaker connections between groups generate holes in social structures, or simply Structural Holes, which create competitive advantage for actors whose relationships span those holes. A Structural Hole is an opportunity to broker the flow of information between actors, and to control the projects that bring those actors together from opposite sides of those holes. In this sense, holes can be understood as buffers, allowing actors, on either side of the Structural Hole, to circulate in different flows of information. Furthermore, it helps separate nonredundant sources of information, that is, sources that add information instead of overlapping information. In Burt's view, Structural Holes and Brokerage are sources of Social Capital in that "individuals with contact networks rich in Structural Holes are the individuals who know about, have a hand in, and exercise control over, more rewarding opportunities" (BURT, 2001, p. 7). Figure 2 shows groups of individuals divided by Structural Holes.

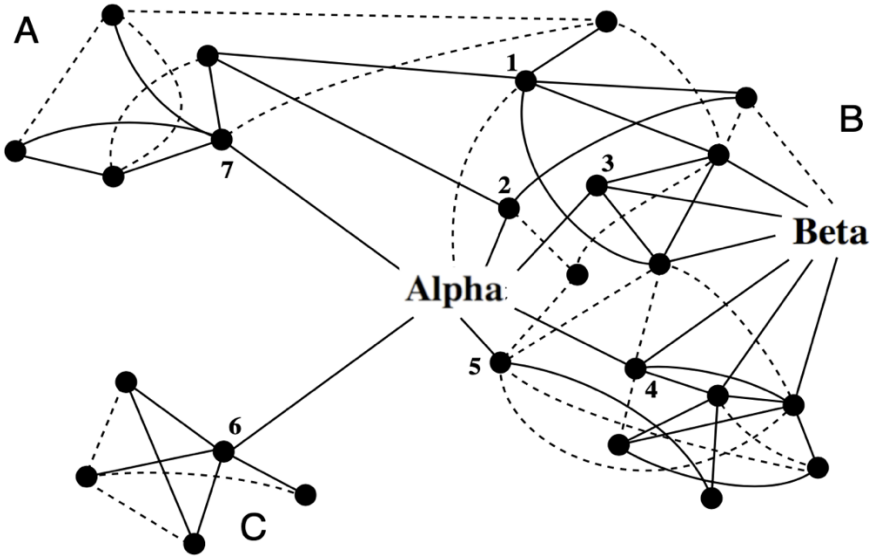


Figure 2: Structural Holes (adapted from BURT, 2001).

In Figure 2, groups A, B and C are aware of each other, but they are focused on their own activities and do not take part in the activities of the other groups. As we can see, Alpha and Beta have the same volume of connections, six strong ties (represented by solid lines) and one weak tie (represented by doted lines), but Alpha has an advantage. Beta is tied to actors within group B, and through them to "connections of connections" all within group B, so Beta is well informed about cluster B activities. Alpha is also tied through "connections of connections" to everyone within group B, but in addition, its strong relationship with connection "7" is a conduit for information on group A, and its strong relationship with "6" is a conduit for information on group C. Its relationships with "7" and "6" meet the SNA definition of a network bridge. If these relationships break, there is no longer a connection between groups B and C. Alpha is thus considered a broker in the network. Its bridge connections to other groups give it an advantage with respect to information access. Alpha reaches a higher volume of information because it reaches more actors indirectly. Furthermore, the diversity of its contacts across the three separate groups means that its higher volume of information contains fewer redundant bits of information. Alpha is positioned at the intersection of the social structure, so it learns about activities beforehand in the three groups. In Sociology, Alpha is called a *tertius gaudens* (meaning, "the third who benefits"), an entrepreneur who benefits from brokering the connections between others (BURT, 2001).

Closure is another network structure that creates Social Capital. Burt (2001) defines a network with closure as one in which everyone is connected, and no one escapes unnoticed by

others. In such context, a closed network acts as a source of information inherent in social relations, in that an actor “saves time” by getting information of important events from a connection, for instance. Likewise, information does not lose quality by being channeled through intermediaries. In this view, direct connections improve communication in a network. This type of structural property of social networks provides the creation of a dense network, which is understood to create Social Capital. Figure 3 shows a closed network in which each entity has ties with all entities in the network.

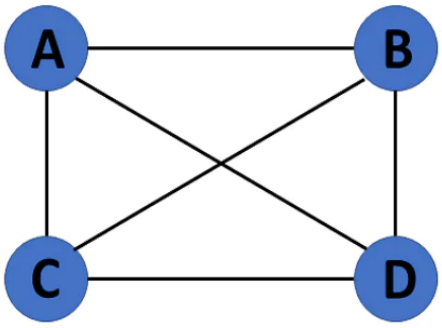


Figure 3: Example of Closure (SIMPLILEARN, 2022).

According to Coleman (1988), Closure can be understood as a property of social relations, in which effective norms supported by sanctions constitute a powerful form of Social Capital. This form of Social Capital not only facilitates certain actions, but also constrains other actions. In this sense, norms arise as attempts to limit negative external effects or encourage positive ones. Closure is important for trust and trustworthiness, which allow the proliferation of obligations and expectations, and reciprocity. “Reputation cannot arise in an open structure, and collective sanctions that would ensure trustworthiness cannot be applied. Thus, we may say that closure creates trustworthiness in a social structure” (COLEMAN, 1988, p. 107). In this light, a network closure of strong ties enables sanctions that make less risky for actors to trust one another.

Bridging and Bonding Social Capital

In the extensive literature on Social Capital, the Structural Hole and Closure approaches relate, respectively, to the Bridging and Bonding dimensions of Social Capital, which are found within social networks and perform different functions. Bridging social capital networks are outward looking and include actors from diverse social cleavages. They are good for linking external assets and for information diffusion, as a way of *getting ahead*. Whereas Bonding social capital networks are inward-looking and tend to reinforce exclusive identities and homogeneous groups. They are useful when reciprocity and solidarity are needed for *getting by* (PUTMAN, 2000).

Burt (2001) points out, however, that the theoretical approaches of Closure and Structural Holes are not mutually excluding and can be brought together in a productive way. He posits for integrating results across studies with respect to empirical evidence, while the mechanisms remain distinct. A study can present exclusive evidence of Social Capital from network closure, or structural holes, without calling into question either argument. When it comes to network effectiveness, Closure describes how dense, or hierarchical, networks lower the risk associated with transaction and trust, while Structural Holes are opportunities to add value with brokerage and bridges across holes. The author's study on performance was able to identify that network effectiveness is the highest when in-group closure is high and there are many non-redundant contacts beyond the group. On the other hand, effectiveness is the lowest where in-group closure is low and there are few non-redundant contacts beyond the group.

It is important to highlight how trust features as an important relational property of Closure and Structural Holes. Trust here is a source of Social Capital in these network structures. Traditionally, researchers on Social Capital argue that closure lowers the risk of trust, since trust is more likely to appear in strong ties, especially if they are embedded in a closed network. The more closed the network, the more likely misbehavior will be detected and dealt with. This leads to preservation of one's reputation, which is built on trustworthy relationships. Coleman (1988) asserts that the presence of trust, as a source of Social Capital, permeates relations and makes sure for actors that obligations are held and will be repaid eventually. In this way, the density of obligations in a given social structure amplifies the availability of tangible resources that can be used by others when needed.

According to Burt's (2004) understanding of network Social Capital, trust is needed to realize the value of bridging a structural hole, while network closure is needed to ensure trust.

The author points out that closure secures a bridge where brokerage creates value as it enhances coordination across structural holes that could otherwise be closed to advantage.

Relational Embeddedness

Trust in strong ties is created by repeated interaction over time, which makes one more confident on the tendency of the other to cooperate. The repetition of cooperative exchange promotes trust, in that past tentative exchanges move towards familiarity in the present, and into more significant exchanges in the future. This accumulation of trust is fueled by people learning to better predict probable behavior, not only whether the other person will cooperate or not, but if it is something that is likely to come to fruition. This type of relation is called "relational embeddedness" (GRANOVETTER, 1985), in that trustworthy behavior is a regularized part of relationships, in which actors prefer to deal with those they had already dealt before, since the information they have on their partners is richly detailed and probably accurate (BURT, 2004).

The network theoretical approaches of Structural Hole and Closure are widely employed in the analysis and evaluation of Inter-Organizational Networks, especially when it comes to network effectiveness. Besides, trust, as a relational source of Social Capital, creates ties that can foster cooperation in Inter-Organizational Networks. Below, a table summarizing Structural Hole and Closure properties together with Social Capital:

Table 3: Closure and Structural Hole properties

Closure	**Structural Hole**
Bonding Social Capital	Bridging Social Capital
Norms, sanctions, obligations	Brokerage
Strong Ties	Weak ties
High density network	Low density network
Thick trust	Thin trust
Redundant information	Non-redundant information

1.3 An Inter-Organizational Network Approach to Interagency

In this report, we discuss interagency cooperation through the lenses of the network approach, and thus it is important that we first understand what interagency means. The term interagency is commonly used in activities that require collective action, that is, a set of public

and private actors working towards a common goal, which usually takes place in a multiplex environment, such as the security field. It is useful to distinguish interagency from the term multi-agency, which means that agencies are aware that they share concerns on the same issues and consider working together, whereas interagency implies at least some degree of interdependence and commitment (CANTON, 2016).

Interagency activities, or working, arise from the need for public agencies and stakeholders to span boundaries and work across sectors to address a myriad of complex and challenging issues that call for the resources and expertise of different agencies. In this context, adopting a "bottom up" or "top down" approach to public administration usually deems ineffective (CONNOLLY et al., 2020).

Interagency workings are generally depicted under the umbrella terms of New Public Management and Collaborative Governance (CONNOLLY et al., 2020). This latter is understood as a governing arrangement, in which public actors engage with non-state stakeholders in a formal, deliberative, and consensus-oriented collective decision process aiming at developing or implementing public policies or manage public programs or assets (ANSELL; GASH, 2007).

Interagency activities involve agencies and stakeholders sharing resources, on a continuum of cooperation, coordination and collaboration (see figure below), in order to improve outcome for the beneficiaries of services.

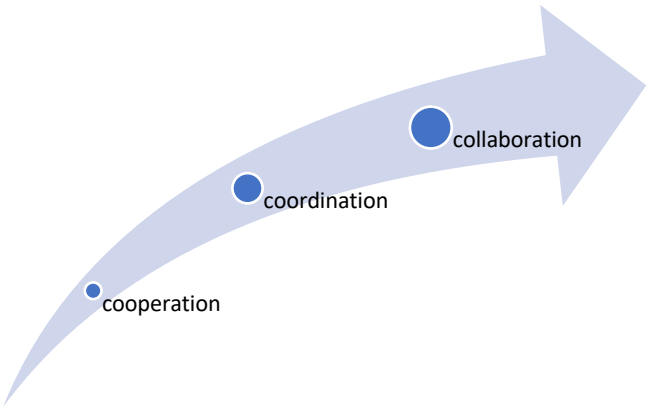


Figure 4: Interagency working continuum.

As agencies move towards collaboration, it implies increasing interdependence, more risks and rewards, as well as stronger commitment and contribution (MACFANWY; ROSIER, 2011). Interagency encompass a multifaceted nature as differing authorities, organizational structures, jurisdictions, legal responsibilities, capabilities, and resources have an impact and

play a role on how agencies work together. When these aspects are clearly defined and in alignment, taking into consideration social related aspects such as trust and organizational cultures, cooperation runs smoothly. On the other hand, when these aspects are unclear, overlap or diverge, cooperation is less effective and sometimes fraught. The increasing role of Interagency working in public administration has brought up a networked-based mentality with regards to policy formation and implementation.

> "The opportunities presented by governing through these networks include the application of complementary skill-sets across the various organizational entities, the forging of bespoke and focused policy initiatives, devolution of power and authority, and the prioritization of public value. The challenges are considerable, however, and include the need for appropriate mechanisms of accountability, and the requirement to strike the correct balance between delegated power and authority on the one hand, and strategic coordination on the other, which emphasizes the importance of genuine collaboration and partnership working, as well as the crucial requirement for strategic political leadership." (CONNOLLY et al., 2020, p. 536)

In the next sections of this report, we discuss an inter-organizational network approach to interagency as a means to foster cooperation. Our aim is to present an detailed view on the advantages and challenges of the network-based mentality as a means to support the development of new public policy agendas and strategies geared towards interagency activities in the security field.

1.4 Inter-Organizational Networks

In this section, we discuss some key themes on Inter-Organizational Networks, such as their purposes; types and functions; advantages, challenges, and limitations; structure and Social Capital; governance; and effectiveness. The themes discussed in this section will help us better comprehend the purposes and properties of Security Networks, and how they can foster interagency cooperation.

Inter-Organizational Networks can be defined as "a group of three or more legally autonomous organizations that work together to achieve not only their own goals, but also a collective goal" (PROVEN; KENIS, 2008, p. 231). The term network is understood here as a form of multi-organizational governance in contrast to hierarchies and markets

(POWELL,1990, *apud* BARDACH, 2017). Compared to hierarchies and markets, networks are more flexible and driven by expectations of trust and reciprocity, in the short and long terms, making them more efficient in eliciting cooperation, resources exchange and mobilization, capacity acquisition, and managing risks (BARDACH, 2017).

In Public Management literature, networks are characterized by different types and their respective functions, as shown in table 4 below. These characteristics usually overlap in real network formations, since they are not static structures and are constantly evolving.

Table 4: Public Management Networks (adapted from MILWARD; PROVAN, 2006)

Network Type	**Key Functions**
Service Implementation Networks	• Government funds the service under contract but doesn't directly provide it. • Services are jointly produced by two or more organizations. • Collaboration is often between programs of larger organizations. • Horizontal management of service providers is a key task. These can be firms, nonprofits, or government agencies. • Key management tasks include encouraging cooperation, negotiating contracts, planning network expansion, etc.
Information Diffusion Networks	Horizontal and vertical ties between interdependent government agencies. • Primary focus is sharing information across departmental boundaries. • Commonly used for disaster preparedness and other "high uncertainty" problems. • Key network goal is to shape government's response to problems through better communication and collaboration. • May be either designed or emergent.
Problem Solving Networks	• Primary purpose is to help organizational managers set the agenda for policy related to a critical national or regional problem. • Focus is on solving existing complex problems rather than building relationships for future problems. • Often emerges from information diffusion networks. • Relationships may be temporary, to address a specific problem, and then become dormant after the problem is resolved. • May be either mandated or emergent.
Community Capacity Building Networks	• Primary goal is to build social capital in community-based settings. • Network purpose is both current and future oriented.

	• May be created by participants (bottom-up) or by private and government funders (top-down). • often involves a wide range of agencies with many emergent sub-networks to address different community needs that may arise.

The advantages of networks are manyfold and include enhanced information and knowledge share, advanced learning, more efficient use of resources, adaptability, reliability, and increased capacity to plan and tackle complex, or "wicked" problems (O'TOOLE, 1997 *apud* PROVEN; KENIS, 2008), that is, problems that cannot be addressed by one single organization and that require collective action between different organizations (PROVEN; KENIS, 2008).

> "The reason 'wicked' problems typically warrant a network response is the need to be highly adaptive (because the problem and/or solution is either unknown, inconsistent, or frequently changing) and because the resources, knowledge, and solutions are spread across many different entities, necessitating a coordinated response from a multitude of organizations. When these conditions exist, networks are generally more effective than either a market or a hierarchy" (PROVEN; LEMAIRE, 2012, p. 641).

It is important to highlight that network is not necessarily a synonym to the concepts of collaboration, partnerships, and collaborative governance. Networks focus on the multiple relations that exist (or not) among a set of actors. Collaboration, for instance, can be an essential element of a network, but it does not necessarily make the network, since not all participants need to collaborate with one another for a network to exist (PROVEN; LEMAIRE, 2012). However, some research on Public Administration identifies three broad types of networks named "Policy Networks", "Governance Networks", and "Collaborative Networks". Here "Collaborative Networks" refer to "agencies that work together to provide a public good, service, or 'value' when a single public agency is unable to create the good or service on its own" (see more in ISETT et al., 2011). Nonetheless, interaction among network participants requires some sort of cooperation, which is defined below:

> "Cooperation refers to the act of working jointly with others, usually to resolve a problem or find a corner of activity. It can be occasional or regular, or it can occur within, between, or outside formal organizations. Here the interest is

> focused on the activities of individuals who represent organizations working across their boundaries" (AGRANOFF, 2006, p. 56).

As will be discussed ahead in this section, in most Inter-Organizational Networks, one important tie that can make up the relational structure of the network is cooperation, which in turn enables the flow of resources.

Before we go further describing the next theme, it is important first to acknowledge why and when to use networks, and what are their challenges and limitations. Scholars of Public Administration have long understood that a Bureaucracy, the classic hierarchy form, is appropriate for stable and routine tasks, but not for handling most nonroutine tasks. On the other hand, "wicked" problems warrant a network response in the sense that networks are highly adaptable and flexible and therefore more suitable for when the problem or solution is either unknown, inconsistent, or frequently changing. Moreover, networks allow a coordinated response from different organizations and the pooling of resources, information and knowledge, which are spread across different organizations, who need to achieve a collective goal. When these conditions occur, usually a network response is more effective than markets or hierarchies (PROVAN; LEMAIRE, 2012). Government authorities worldwide employ the network approach as a strategy to fight terrorism and disrupt the illicit activities of organized crime (RAAB; MILWARD, 2003), which fall outside the boundaries or mandate of individual law enforcement organizations, and thus require a coordinated effort and cooperation among agencies. More on that in the coming section of this report on Criminal Networks and Security Networks.

While the reasons and advantages of networks are many, they are not without challenges and limitations, such as culture clashes, difficulty achieving consensus on network purpose and goals, coordination fatigue, complex management and leadership, cost and budget, time and effort to develop trusting relationships, power imbalances, and so on. Besides, cooperation among organizations in a network is considered paradoxical, since on one hand it can promote consensus, communication, sharing of knowledge and goals, but on the other there exits the reality of competition, conflict, differing organizational autonomies and cultures (PROVAN; SYDOW, 2007).

Researchers on networks suggest weighing in the added benefits of networks to its challenges, in a given circumstance. The degree to which challenges can be foreseen, managed or circumvented is an important consideration when establishing networks. Thinking about the challenges can also help determine the composition of the network design and governance to

ensure its effectiveness (POPP et al., 2014). Below, two tables summarize the advantages and challenges of Inter-Organizational Networks.

Table 5: Inter-Organizational Network advantages (adapted from POPP et al., 2014)

Advantage	**Description**
Access to and leveraging of resources	• Stretch, build on or strengthen limited resources. • Access to resources not held within a particular organization.
Shared risk	• The ability to distribute or share risks fosters creativity and innovation by reducing risk to any one organization.
Efficiency	• More efficient use of resources. • Ability to achieve economies of scale (e.g., purchasing, being more competitive in grant competitions).
Service quality, coordination, seamlessness	• Ability to provide coordinated, higher quality services and a full continuum of care.
Advocacy	• Able to exert more pressure due to greater political clout and community reach resulting from greater numbers and diversity of network members.
Learning, capacity building	• Knowledge exchange can enable learning and capacity building at a network level and in the broader community.
Positive deviance	• Networks can be a forum to think and act beyond the organizational norm, structure, or mandate; to work deliberately in deviation from the standard organizational processes, overtly or covertly, to influence change in systems
Innovation	• Networks are enabling structures that create opportunities for innovation, which is closely connected to learning.
Shared accountability	• Opportunity to work collaboratively to address, and share responsibility for, a quadruple bottom line (e.g., financial, social, environmental, and cultural) • Developing a sense of accountability to one's network colleagues.
Flexibility and responsiveness	• Capacity to be more flexible and responsive in order to deal with unforeseen problems (e.g., disasters).

Table 6: Interorganizational Network Challenges (adapted from POPP et al., 2014)

Challenge	**Why it is a challenge**	**How it can be mitigated**
Achieving consensus on and varied commitment to network purpose and goals	Member organizations come to the table with diverging perspectives and priorities, varying levels of trust in the process, and differing tolerance for subjugating individual needs in favor of the common goal.	• Use a participatory, collaborative process for establishing initial goals, making sure to involve key stakeholders and implementers. • Develop specific terms of reference for the goals of the collaboration. • Choose early activities that could change behavior first, contributing to new norms and, ultimately, consensus.
Culture clash, or competing "institutional logics"	Member organizations have different ways of doing things (cultures) and/or institutional logics (e.g., approach to decision making, ways of providing services, transparency with partners), which can make it challenging to agree on essential structures, processes, and outcomes.	• Identify and openly discuss the underlying cultures and logics of member organizations. • Develop structures and processes for the network that reflect a diversity of those found within member organizations.
Loss of autonomy	Legally autonomous organizations may resist coordinated decision-making, particularly when the decisions are not perceived as being in the best interests of their organization.	• Ensure that planning and decision-making is participatory and open. • Pay attention to how a potential decision could affect organizational members differently; highlight the potential gains.
Coordination fatigue and costs, including being pulled in multiple directions	Working collaboratively and coordinating decisions and activities take time and effort away from the day-to-day work of an organization. As well, it is not uncommon for a single organization to belong to multiple networks, which exacerbates the time and effort required.	• Adoption of an appropriate governance form and sufficient resourcing of the network can help ensure that the time individual member organizations commit to network activities is optimized. • Creating a network culture that allows members to engage at varying intensities on particular activities can also provide relief.
Developing trusting relationships	Trusting relationships take time to build and must continue to be attended to if trust is to be maintained over time because reciprocity emerges from repeated interactions.	• Build trust initially by sharing non-threatening information or knowledge and engaging in low-risk activities, thus demonstrating competency, good intentions, and follow-through. • Regular check-ins on the 'health' of network.

		Relationships may help identify and mitigate trouble. • Use the strategy of tit for tat; if someone cooperates with you in the first round, you cooperate with them in the next. • Cooperate with a non-cooperator occasionally as they may surprise you and cooperate.
Obstacles to performance and accountability	Accountability can be a particularly complex issue, as it is often not clear to whom the network is accountable and for what. This diffusion of accountability can lead to "free-riders", where some organizations participate minimally and let others pick up the slack.	• Establish an early expectation that all network members will contribute in some fashion over time, setting the stage for network members to hold each other accountable. • Tracking inputs and creating transparency within the network can also make individual member contributions and corresponding outcomes more visible and provide evidence for tough conversations with "free-riders".
Management complexity	Management within a network context requires managing across organizations as well as within the traditional hierarchical structures of member organizations. Tensions that arise between the two are typically difficult to resolve but still require confronting.	• Acquire and share knowledge within the network about how networks operate. • Identify how each organization fits into the network and predict the tensions that may arise. • Ensure good conflict resolution mechanisms are in place to address issues in an open and transparent way. • Foreshadow the fact that some tensions may be irresolvable and that this is acceptable within the network culture.
Power imbalance and resulting conflict	As in life, organizational members come into the network with differing levels of status and resources, making power imbalances a reality.	• Use language that reinforces equality among members. • Provide early and ongoing assurance that the interests of all members are being considered. • Use resources to mitigate power imbalances and manage conflict effectively.
Lack of organizational capacity to work collaboratively	Organizational members may lack experience working collaboratively because of	• Work to develop the network culture or a compelling

	traditional organizational ways of working.	narrative such as the 'network way of working'. • Provide education on collaboration to network members. • Choose an early activity to work together on that has good potential for a quick win. • Model a collaborative leadership style.
Sustainability	Sustaining a network can be challenging for a number of reasons, many of which have been discussed throughout this table. An additional challenge to network sustainability is change in the environment within which a network operates, or the network moving to a new evolutionary stage of development.	• Ensure the network remains nimble by trying to anticipate and respond/adapt to changes in context • Promote network level learning. • Institutionalize network structures and processes to encourage stability.

1.4.1 Network Structure and Social Capital

Organizational Network scholars argue that a comprehensive understanding of network structure can assist in the optimal governance design to ensure a more effective network. The Inter-Organizational network themes of structure, governance and effectiveness are interlocked as will be shown in the following sections of this report. To study network structure, scholars make use of SNA methodologies and theoretical approaches to understand actor position, the relational patterns (e.g., cooperation) and processes (flows) that occur within the network. Two methodological-analytical perspectives are used: Egocentric and Whole Networks. (PROVEN; LEMAIRE, 2012).

The Egocentric perspective analyses the individual organization's position and dyadic ties with other actors in the network, focusing on the benefits or other outcomes (possibly negative). The Whole Network perspective shifts the focus from a micro approach (the ties that an actor has) to a macro approach (all ties, present and absent, among a set of actors). Research on Whole Networks provides important information on how networks are governed, its effectiveness, and how actors cooperate to achieve a common goal. This is vital for policy planners and those who work within a perspective that goes beyond the individual performance of organizations. It is important to note that while the analytical distinctions between Egocentric dyadic ties and Whole Network multilateral ties are clear, from a methodological viewpoint,

understanding how Whole Networks operate requires consideration of the dyadic ties maintained by individual actors (PROVAN; SYDOW, 2007).

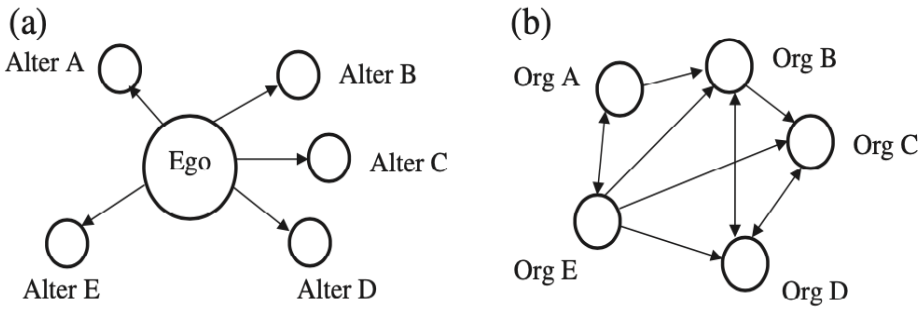


Figure 5: Egocentric (a) and Whole Networks (b) perspectives (PROVEN; LEMAIRE, 2012).

The concept of Social Capital features prominently in Inter-Organizational Network research. When forming network ties, organizations benefit from the advantages of Social Capital (PROVEN; LEMAIRE, 2012). Organizational scholars apply the concept of Social Capital to better understand issues related to cooperation in networks as an indicator of social strength (which actor is in the center of the cooperation activity), trust and reciprocity, resource mobilization (who has access or control of the flow of resources, e.g., information exchange), both at Egocentric and Whole Network perspectives.

As seen in the previous section 1.2 of this report, the network structures of Structural Holes and Closure are better at creating Social Capital, and in Whole Network research, Social Capital holds an effect that some network formations are more effective than others in advancing cooperation based on trust and reciprocity. In other words, in network formations of Structural Holes and Closure, trust is an essential relational source of Social Capital that helps foster cooperation, which in turn improves network effectiveness (BURT, 2004; WHELAN, 2017)

The Closure approach correlates trust with strong relationships, in which past cooperation forms the basis for future cooperation. A history of repeated cooperation between actors strengthens their relationship, increasing the chances that they trust each other. On the other hand, if they have a history of erratic cooperation mixed with exploitation, or a history of consistent failure to cooperate, they will probably distrust one another and avoid cooperating in future endeavors, since there is no guarantee on how the other will behave. When it comes to brokerage opportunities in weak relationships, trust also plays a crucial role, since the Social

Capital of Structural Holes also depends on trust. Here, trust lies in the anticipated cooperation and is more critical when brokerage is more valued, such as when actors deal with task ambiguity. In this context, data is less important than the colleagues you know, since what you know is unclear or out of date, and who you know is the only available path to stable certainty (BURT, 2004).

1.4.2 Network Governance, Management, and Leadership

Network governance is an interlocking theme to network structure since it is an important task for network managers to determine which type of governance is a best fit for a given network to ensure effectiveness at a particular time. First, it is important to distinguish what are Mandated or Goal-Oriented Networks and Serendipitous or Emergent Networks. Goal-oriented networks refer to formal mechanisms designed to coordinate organizations for the purpose of achieving individual and collective goals. In the public sector, networks are usually goal-oriented in the sense that they may be mandated by government or initiated by government departments or agencies. Serendipitous networks refer to informal or emergent networks that develop not by design but randomly. Such networks may take place within goal-oriented networks or may take an entirely separate trajectory (PROVEN; LEMAIRE, 2012).

Provan and Kenis (2008) define Network Governance as "the use of institutions and structures of authority and collaboration to allocate resources and to coordinate and control joint action across the network as whole" (PROVAN; KENIS, 2008, p. 230). The authors propose a typology to categorize network governance that is widely recognize in Public Administration literature as an important contribution to network effectiveness. The types are: Shared Governance; Lead Organization; and Network Administration Organization (NAO).

In "Shared Governance", networks are completely governed by the organizations that comprise it, in a dense and highly decentralized fashion, with no separate and unique governance entity. This governance type is generally acknowledged to be challenging when the network is made up of a large number of organizations (usually more than 5 or 6) (PROVAN; LEMAIRE, 2012). In "Lead Organization", governance is the responsibility of a single organization in the network that acts as a highly centralized broker, which is in charge of key decisions and all major network-level activities. The third form of network governance, "Network Administrative Organization" (NAO), takes place at mid-range, where a single organization may be in charge of key governance roles, leaving other network members to divide responsibilities by working in groups, or cliques. In NAO, the lead organization is not a

member of the network, but an external entity, established through mandate, or by the members themselves, for the exclusive purpose of governance (PROVAN; KENIS, 2008).

Table 7: Types of Network Governance (adapted from PROVAN; KENIS, 2008)

Governance Type	**Description**
Shared Governance, consensual	All participants contribute to the management of and leadership in the network. There is no formal administrative entity.
Lead Organization	The network manager and administrative entity is one of the key network members.
Network administrative organization (NAO)	A separate administrative entity is established to manage the network, and a manager hired.

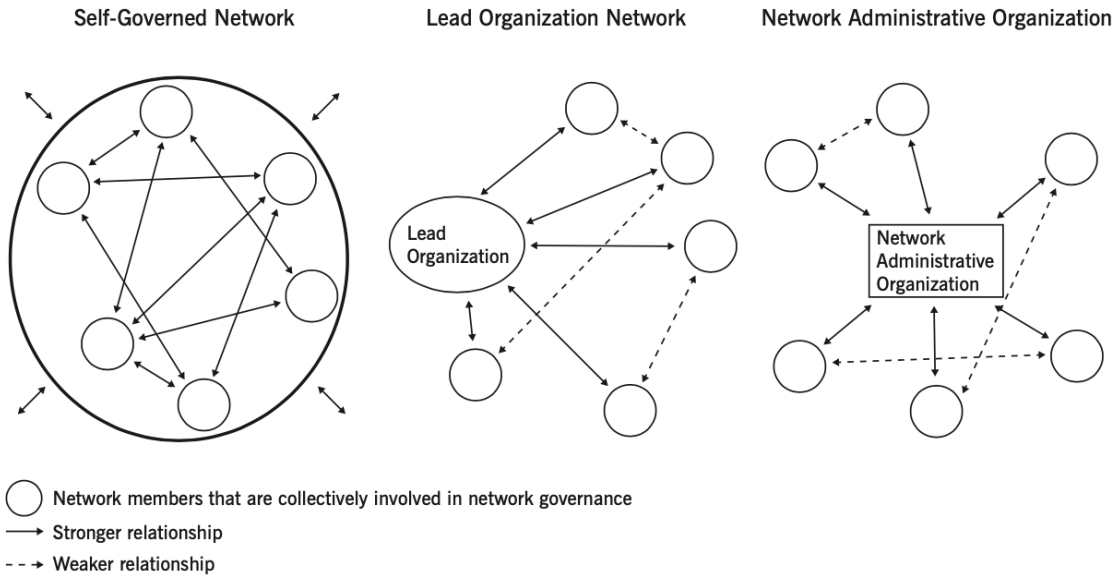


Figure 6: Structural Design of Network Governance typology (POPP et al., 2014).

More recently, researchers on Public Administration argue that network governance may entail a hybrid format involving more than one type. Empirical research on Inter-Organizational Network governance points out that formal governance mechanisms, e.g., contracts, can be complementary to inter-organizational trust. Research also highlights the fundamental challenge to governance is that the needs and activities of multiple organizations often require accommodation and coordination to curb tensions within the network, such as possible resources and budgetary constraints (POPP et al., 2014).

Regarding network management, Agranoff (2006) conducted an empirical study involving 14 public networks, in which virtually all of the networks studied operated with some sort of council or board elected by the entire set of participants. However, he calls attention for the fact that the real work in the networks was done by committees or focus/short-term workgroups. These committees usually try to reach agreements on technical merits and possibilities without hierarchical involvement and they also reach out to expertise (and possibly resources) inside and outside the network wherever can be found. So, for a network to thrive it is crucial for network managers to ensure that the network is adequately resourced if its effectiveness is to be maximized, taking into account network capacity and the evolving nature of networks (POPP et al., 2014). Below a table summarizing some network management tasks and behaviors.

Table 8: Inter-Organizational Management (POPP et al., 2014)

Network management task or behavior	**Description**
Framing	Facilitating agreement on the operating rules of the network, including its prevailing values and norms; developing a shared vision; helping establish an identity and culture for the network; helping establish a working structure for the network.
Activation; construction of the right community	The identification and incorporation of the right mix of people or organizations to achieve program goals, as well as ongoing building of member capacity.
Management of design/governance structure	Selecting a governance structure that is likely to work most effectively for the network, and then ensuring that the structure evolves appropriately with the network.
Creating and supporting participatory leadership	Building leadership for collaborative advantage; providing opportunities for distributed or shared leadership; developing consensus on vision; using influence; creating a welcoming culture; etc.
Synthesizing, facilitating, involving, arranging, connecting	Creating the environment for productive interaction among network participants. Organizing interactions; facilitating relationships in order to build trust.
Development and flow of resources	Includes the development of both material (e.g., funding, human resources) and tacit resources (e.g., knowledge, new practices), and decentralizing the flow of these resources.
Management of commitment; mobilizing	Building commitment for the joint undertaking, sometimes also referred to as mobilizing. Dealing promptly with the perception or reality of unequal distribution of resources in the network or unequal commitment to the network,

	as well as training and joint problem-solving exercises, can help in building commitment.
Facilitating knowledge exchange; collaborative dialogue	Aim is to establish a knowledge base that can be used by the network to address complex problems, so a key role for managers is to build this capacity across the network. Involves actively exploring the different views of participants and connecting these ideas.
Management of conflict	Listening to the various voices of members and providing mechanisms for conflict resolution; bridging differences through mediation; providing opportunities for open dialogue and structured disagreement.
Management of accountability	Key issues include who is responsible for what; how to respond to free riders; how to measure joint success and attribution of value.
Management of legitimacy	Working to convince stakeholders, both internal and external to the network, that working with other organizations in broader network is worthwhile. This involves building support both internally and externally. This is closely related to management of commitment and mobilizing.
Management of tensions; paradoxes	The management of tensions, including tensions that arise related to the governance structure selected, organizational culture, trust and cooperation issues, is critical for explaining network effectiveness.
Promoting network level learning	Shared learning by individuals from the group of organizations in the network. The collective learning advances the network culture, collective knowledge and understanding of the network. For example, bringing network members together to learn about networks, simultaneously and from the same information and experience, helps advance the common culture of the network. This is distinct from the network as a context for individual learning on varied topics of interest to the network or its organizational members.

Leadership within network management is considered a challenging task since it is people (representatives of organizations) who cooperate with one another. Therefore, a successful collaborator must be concerned with the needs and interests of her/his organizations and the goals of the network. For that, she/he must recognize the benefits of synergy with other collaborators in the network, taking into account organizational culture, mandates, and values of each participant organization. Scholars of network governance identify four leadership roles, they are (POPP et al., 2014, p. 43):

- Connector catalyst: connecting people and helping to get network started.

- Project Coordinator: helping network members with their self-organized projects of interest.
- Network Facilitator: helping with ongoing development of network structures, activities, and relationships.
- Network guardian: putting in place systems such as communications, training, and resources to help networks as whole function effectively.

1.4.3 Network Outcome – Effectiveness and Evaluation

The key factor that sustains networks is effectiveness, which is achieved by working together rather than separately, that is, through cooperation/collaboration. In this light, there has been a growing number of studies focusing on network outcome of effectiveness at the Whole Network level. According to Provan and Kenis (2008, p. 230), "network effectiveness can be defined as the positive outcomes that could not normally be achieved by individual organizations participants acting independently." Effectiveness is a difficult concept to define and is often used interchangeably with performance. Some scholars define it as the ability of organizations to perform effectively and efficiently. Other scholars understand effectiveness as a measure of quality of output, while efficiency as quantity of outputs (WHELAN, 2017).

Based on network interactions, Provan and Kenis (2008) identify certain critical contingencies based on network structure and relations that signal if a particular form of governance is likely to be effective. They are: Trust; Size; Goal Consensus; and Need for Network-Level Competencies. The distribution of trust is critical, whether it is reciprocated or not, among network members. For instance, in high density networks, trust is widely distributed, and in low density networks, it is narrowly distributed taking place in different manners within dyads or cliques. Shared Governance, for instance, becomes an effective form when trust prevails throughout the entire network. Trust does not to be deep, but it cannot be contingent simply on a collection of dyad-based relationships. Besides, trust must be dense so that the perception of trust is shared among all network members. On the other hand, when low density trust is prevalent in a network, it can still be a viable way of achieving effectiveness in collective goals when the network is likely to be brokered, either through Lead Organization or NAO (PROVAN; KENIS, 2008).

A fundamental challenge of network governance is that the needs and activities of participants must be accommodated and coordinated. As the number of participants grows, the number of potential relationships increases exponentially, making governance an extremely

complex task. And so, the structural solution might be to centralize network governance activities around a Lead Organization or a NAO. Goal Consensus is also a challenge in the sense that network participants must be responsive to the specific goals of their individual organizations and the collective goals of the network, especially in mandated/goal-oriented networks. In this view, there may be considerable variance across members on network goals and the extent to which individual organization goals may be achieved through network involvement/interactions. The critical issue here is how relationships are governed. To be effective, in Shared Governance, goal consensus must be high, that is, the organizations must all agree on network goals, whereas in Lead Organization, it can be moderately low (PROVAN; KENIS, 2008).

Finally, when it comes to the need for network-level competencies, organizations join in or form networks usually as a means to achieve some end goal that they could not have achieved independently. The question that arises thus is how to attain the competencies required to achieve such collective goal? Two issues are key in this matter: the nature of the task being performed by network members, and the type of external demands and needs faced by the network. For instance, if the network task requires significant interdependence among participants, then the need for whole network coordination skills will be great, meaning the governance will need to facilitate such actions, and so Shared Governance might not be the optimal form, since it might put pressure on individual organizations demanding skills that they may not have. In this case, Lead Organization or NAO will be better suited (PROVAN; KENIS, 2008).

In general, the authors argue that as the number of participants in a network increase, trust becomes less densely distributed, and the goal consensus declines. Moreover, as the need for network-level competencies increases, a brokered form of governance, such as Lead Organization or NAO, becomes more effective than Shared Governance. Below, a table summarizing network governance contingencies.

Table 9: Contingencies for governance effectiveness (adapted from PROVAN; KENIS, 2008)

Governance Type	**Trust**	**Number of Participants**	**Goal Consensus**	**Need for Network-Level Competencies**
Shared Governance	High Density	Few	High	Low
Lead Organization	Low Density (Highly centralized)	Moderate number	Moderately low	Moderate

Network Administrative Organization (NAO)	Moderate density (monitored by members)	Moderate to many	Moderately high	High

Regarding network evaluation, the single most valuable methodological tool available to network evaluators is Social Network Analysis. In Organizational Studies, SNA offers a holistic view of the network, when usually only parts of that network are familiar to its actors. An accurate view of the network is a source of power, which can enable better cooperation. SNA may be employed for evaluative purposes as a diagnostic tool to identify network formation, relations, and central actors, highlighting intervention points by signaling gaps or bottlenecks. Similarly, it can be used to understand which parts of the network are working well, and other that are not, and it can also be employed by qualitative research to comprehend the contextual conditions and mechanisms that enable effective operations (BRUN; MCAULIFFE, 2018). In this light, SNA can be used as an evaluative tool to make recommendations and improve network cooperation, mobilization, and exchange of resources, based on insights and observations into relationships among network members.

Social Capital can be an important variable when evaluating network effectiveness especially concerning cooperation based on trust and reciprocity, as discussed previously in this report. Borgatti et al. (1998) describe measures used to formalize the analysis of Social Capital in networks. The authors identify two forms of Capital Social, one related to individual actors (Egocentric) and the other to Collective actors (Groups or Whole Networks), and their respective measures. The tables below summarize the measures for Egocentric Social Capital and Whole Network Social Capital.

Table 10: Egocentric Measures of Social Capital (adapted from BORGATTI et al., 1998)

Name	**Description**	**Relation to Social Capital**
Size/degree	The number of alters that an ego is directly connected to, possibly weighted by strength of tie.	Positive. The more people you have relationships with, the greater the chance that one of them has the resource you need.
Density	The proportion of pairs of alters that are connected.	Negative. If all your alters are tied to each other, they are redundant.
Heterogeneity (requires attributed date on nodes)	The variety of alters with respect to relevant dimensions (e.g., sex, age, race, occupation, talents).	Positive (except when it conflicts with compositional quality).

Compositional (Quality)	The number of alters with high levels of needed characteristics (e.g., total wealth or power or expertise or generosity of alters).	Positive. The more connected to useful others, the more social capital.
Effective Size	The number of alters, weighted by strength of tie, that an ego is directly connected to, minus a "redundancy" factor.	Positive. The more different regions of the network an actor has ties with, the greater the potential information and control benefits.
Closeness	The total graph theoretic distance from ego to all others in network.	Negative. The greater the distance to other nodes, the less the chance of receiving information in a timely way.
Betweenness	The number of times that ego falls along the shortest path between two other actors.	Positive. Actors with high betweenness link together actors who are otherwise unconnected, creating opportunities for exploitation of information and control benefits.
Eigenvector	The extent to which ego is connected to nodes who are themselves high in eigenvector centrality.	Positive. An actor has high eigenvector scores when they are connected to well-connected others.

Table 11: Whole Network measures of Social Capital (adapted from BORGATTI et al., 1998)

Name	**Description**	**Relation to Social Capital**
Density	The proportion of group members who are tied (with a "positive" relation, such as friendship, respect, acquaintance, past collaboration, etc.).	Positive. Curvilinear for intellectual conflict relations; Negative for personal conflict relations.
Average or maximum distance	The average (or maximum) graph-theoretic distance between all pairs of members.	Negative: Smaller distances mean faster communication among members, which is an asset.
Centralization/Core-Periphery Structure	The extent to which the network is NOT divided into cliques that have few connections between groups.	Positive. Controlling for density, core- periphery structures are easier to coordinate than fractionated networks.
Homophily (requires attributes on all the nodes)	The extent to which members of the group have their closest ties to members who are similar to themselves.	Negative. Less homophily should mean greater exposure to a wider range of ideas.

Another important variable for network effectiveness is Organizational Culture, which has also an important impact on cooperation and network performance. According to Whelan (2016), organizational cultures that exist in each network can either yield positive outcomes or

negative ones, in the sense that conflicting organizational cultures may cause problems for networks in relation to different outlooks, mindsets, and goals. Cultural differences can thus undermine cooperation having a direct impact on network effectiveness. It is therefore important to consider the way in which organizational cultures shape the network and how networks shape organizational cultures.

Social Capital and Organizational Culture, as network variables, converge in terms of trust playing a strategic role in close interpersonal and inter-organizational relationships that instill commitment and reciprocity, which facilitate the development of communities of practice aimed at achieving cooperation towards a collective/common goal. In this light, trust can be achieved *a priori* by shared values and norms of reciprocity, which requires shared culture, and it can also be developed within the relationship, which entails Social Capital. For both Social Capital and Organizational Culture, trust is pre-requisite to knowledge exchange, as Staber (2003, p. 415) points out "to encourage knowledge exchange one must develop common understanding, which constitutes a relation-specific investment in cooperation". Both concepts also converge on the importance of strong social ties as a venue for organizational cohesion and cooperation. Even proponents of weak ties in Social Capital, as a way of accessing knew knowledge, agree on the importance of developing trust in terms of integrity and synergy (STABER, 2003).

1.4.4 Public Sector Knowledge Networks (PSKNs)

Now that we have covered some of the key themes of Inter-organizational Networks, we present in this section a particular type of network, called Public Sector Knowledge Network (PSKN) (DAWES et al. 2009), which entails a shift from a "need to know" to a "need to share" in Public Administration. Like Information Diffusion Networks described in table 4, this type of network is tailored to provide information and knowledge sharing across organizational boundaries to address complex problems that require collective action. "PSKN are sociotechnical systems in which human, organizational, and institutional considerations exist in mutually influential relationship with processes, practices, software, and other information technologies" (DAWES et al. 2009, p. 392).

PSKNs involve two dimensions: focus and extensiveness. About focus, they can be either "narrow focus", which uses knowledge networking to meet a specific need or problem, or "broader focus", which aims to build systemic capacity to share information and knowledge whenever needed. Narrow focus networks have the advantage of clarity, since all participants aim at an end goal within a pre-defined time horizon. However, such networks lack staying

power and flexibility. On the other hand, broad focus networks are considered more permanent and versatile assets, but more challenging and difficult to implement and sustain its operations, which require increased capabilities, greater budget, as well as the need for an appropriate and enduring organizational home for the network. When it comes to extensiveness PSKNs can be: "intra-organizational" (within a single organization); "inter-organizational within a single government jurisdiction"; and "inter-organizational across jurisdictions, sectors, and levels of government". Although this latter has greater depth and variety of information and knowledge to share, the myriad of actors and stakeholders may represent more organizational and jurisdictional barriers, as well as managerial risks and costs (DAWES et al. 2009).

PSKNs offer an environment to form communities of practice by making use of information systems, communication tools, and data resources to improve actors' processes and practices aimed at a common goal. It is important to note that while information systems play a crucial role in this type of network, they do not ensure network effectiveness without taking into consideration more "subjective" aspects regarding the variety of organizational, sociological, ideological, relational, and political contexts that coexist within such networks.

Overall, PSKN has the potential to offer substantial benefits to its participants as it acts as a communication channel that gives actors access to other actors' information and knowledge in a timely manner according to specific needs. It is important to highlight that information form the basis for knowledge development, whereas knowledge is often required to assimilate and interpret information. The information and knowledge that flows in a PSKN are of better quality, and from a learning perspective it allows connecting to other actors' perspectives, as well as sharing of experiences and practices, which make up a major resource for professional and organizational innovation. Such features of PSKNs help agencies to better prepare and improve their responses to uncertainty and complexity of a given environment. Therefore, shared information and knowledge integration can help agencies to better define their individual goal(s) and common goal(s) to solve complex issues, fostering interagency activities, such as coordination of joint programs, polices and services (DAWES et al. 2009).

In a comprehensive action research on PSKNs, Dawes et al. (2009) identified 13 lessons, regarding challenges, choices, and opportunities (see table below) that are worth considering when designing and implementing this type of network.

Table 12: PSKN's Lessons (adapted from DAWES et al., 2009)

Lesson 1: The elusive nature of knowledge can cause considerable difficulty for PSKNs - it is dangerous to assume that meanings are clear, context is understood, and quality is acceptable to all participants.
Lesson 2: As a potentially sharable resource, knowledge varies in several essential respects - codifiability, embeddedness, and dynamics - and each variation demands substantially different treatment within a PSKN.
Lesson 3: PSKNs are a form of cross-boundary exchange. The boundaries of organizations, jurisdictions, and sectors present the most obvious challenges, but more subtle boundaries related to ideology, professional norms, and institutional divisions can be equally problematic.
Lesson 4: Trust, like knowledge, comes in different forms that work best under different conditions. Lack of sufficient trust—and lack of the right kind of trust—can be powerful inhibitors to PSKNs.
Lesson 5: Risk is inevitable in PSKNs, and it is perceived and handled differently by different players.
Lesson 6: The processes of PSKN engagement build professional networks, organizational connections, and reusable capabilities regardless of the level of substantive network success.
Lesson 7: Acquiring legal authority for a PSKN is a necessity, but there is no one-size-fits-all approach to structuring formal authority. Regardless of structure, mobilizing political support really helps.
Lesson 8: Policy barriers are the greatest obstacles to substantive success in building PSKNs, but often they can be navigated by early intervention, focused action, and consistent attention.
Lesson 9: Organizational barriers are serious, but amenable to innovation and creative management.
Lesson 10: Multiple leadership behaviors are associated with success, including mission focus, emphasis on people and communication, willingness to experiment, and nurturing a culture of joint responsibility for success.
Lesson 11: Early experience sets the tone and direction of cross-boundary relationships— unrealistic, incorrect, or misaligned expectations, processes, incentives, and assumptions are hard to change once set.
Lesson 12: Learning and adaptation are essential to PSKN development and survival.
Lesson 13: Technology is necessary but not sufficient for success.

1.5 Dark and Bright – Criminal Networks and Security Networks

In this section, we adopt a network perspective to Security Governance, which involves a shift in mentality and practices from a state-centered approach to security to one involving more pluralistic networked modes of coordination both for organized crime and security responses. First, we present an overview of the characteristics and activities of Transitional Organized Crime (TOC), and how criminal organizations have adopted a network morphology. Next, we present the concept of Security Network as a crucial response to networked criminal activities in a sense that "it takes networks to fight networks" (AQUILLA; RONFELDT, 2001). This network approach to security gained momentum after the 9/11 terrorist attacks, which drastically changed the security landscape, especially in the USA, EU, UK, Canada, and Australia, shifting how security agencies interact with one another and work together.

1.5.1 Criminal Networks

Transnational Organized Crime (TOC) is today a central concern for governments and law enforcement agencies around the world. The illicit activities of organized criminal groups transcend countries' boarders and encompass all profit-motivated crimes including drugs and weapons trafficking, smuggling of migrants, human trafficking, money-laundering, trafficking of counterfeit goods, wildlife, and cultural propriety, and cybercrimes. TOC represents a growing threat to global trade and economy, human security and peace, the environment, and the political stability of some countries by ways of corruption, infiltration in government, and loss of democratic participation (UNODC, 2000). Taking stock of the threats posed by TOC to international security, the UN Convention against Transnational Organized Crime (UNTOC) entered into force in 2003 aiming at promoting cooperation among member states. The states that ratified the instrument are committed to taking a series of measures against TOC.

Despite international efforts made to disrupt its criminal activities, TOC has managed to grow and expand over the last 20 years. Its worldwide pervasiveness is due to the geopolitical, economical, and technological changes brough by globalization. Organized criminal groups have taken advantage of the opening of new markets and supply chain, with the flow of goods, people, and money through borders. It also exploits the weak regulation of financial markets and the lack of transparency of banking systems, as well as the cyberspace. The new technological advancements in communications and finances have empowered this criminal groups and have optimized their illicit activities by concealing them from law enforcement. Social media and other communication technologies allow them to communicate undetected, while illicit financial flows are hidden through money laundering and in tax havens (GI-TOC, 2021).

TOC is known for its adaptability to changing circumstances. It is a dynamic industry, which seeks to exploit novel opportunities and markets as they arise. Research on TOC identified five overarching illicit markets that have expanded and diversified over the last 20 years, and which are interlinked. They are: (1) illicit markets for human exploitation, (2) illicit environmental markets, (3) illicit drug markets, (4) cybercrime, and (5) illicit trade in legal goods (GI-TOC, 2021).

The illicit drug market is a hallmark of TOC and its most lucrative activity. The volume of illegal substances to reach consumer markets all over the globe, through new trafficking routes, has greatly increased over the last years, with markets in Europe and the USA driving most of the demands. Cocaine trafficking is today the biggest and more profitable activity

carried out by TOC, with record manufacturing and seizures by law enforcement around the world.

Although suffering a setback in 2020 due to the COVID-19 pandemic lockdown restrictions imposed by many countries, the illicit drug market has now quickly recovered to pre-pandemic levels. Besides, some trafficking dynamics have accelerated during the pandemics. These include amplified use of waterways and large shipments, especially the use of container ships, as well as increased use of private aircrafts, small vessels, and contactless methods to deliver drugs to end-consumers. The post-COVID-19 economic crises may also expand drug cultivation and production due to food insecurity in some regions and accelerate drug use disorders (WORLD DRUG REPORT, 2021). Furthermore, the ongoing war in Ukraine may affect transnational drug trafficking and its European market and the dynamics of criminal networks in that area over the coming years.

The Illicit Drug Industry

Drug trafficking encompasses an entire industry with its own supply chain. It involves production facilities, protection (security and legal support personnel), transport and distribution, retail, and management of illegal assets (including banking, real-estate development, and money laundering). Additionally, the dark web has facilitated the transaction of and access to illicit drugs and is a growing market worth around $315 million annually (WORLD DRUG REPORT, 2021). The highly profitable illicit drug market generates huge amounts of money and influence, empowering drug trafficking groups and encouraging them to form new alliances with other criminal and armed groups, and political actors. Criminals are also diversifying their portfolio to include human smuggling and extortion, weapons and counterfeit goods trafficking, and other types of lucrative illicit activities (GI-TOC, 2021).

The globalized environment together with advancements in technology and communications have created the ideal setting for networks of criminal groups to operate and flourish. Law enforcement agencies and security organizations worldwide recognize nowadays that TOC operates through fluid networks, rather than other types of organizational structures, such as markets and hierarchies (e.g., the traditional Italian mafia groups). Networks are considered more flexible than hierarchies and more coordinated than markets (GERSPACHER; DUPONT, 2007). Criminal networks, or “dark networks”, are loose associations of criminals, without a clear center of gravity, cooperating to achieve a profit-driven goal. However, some criminal networks may feature some sort of hierarchical element or local leadership (BRIGHT;

WHELAN, 2020). Dark networks operate as boundary spanners, taking advantage of the porosity of borders and differing criminal justice systems of countries to carry out their illicit activities unflinchingly (GERSPACHER; DUPONT, 2007).

Criminal networks are known for their decentralized, redundant, and adaptable nature, making them more resilient to law enforcement disruption efforts. The versatility of networks allows them to change operations rapidly due law enforcement interventions and to quickly exploit new opportunities. Such features of criminal networks differ from the traditional bureaucracies of law enforcement agencies, which entail slow moving operations that hinder timely responses. By assuming a network structure, these criminal groups are not easily neutralized, since the removal of one or more members of the network might temporarily thwart it but will not comprise the functioning of the entire network. (GERSPACHER; DUPONT, 2007; BRIGHT; MALM, 2019).

Network ties rely on horizontal and informal relations, based mostly on trust and casual cooperation between members, instead of hierarchical or bureaucratic processes. Participants, or actors, in these criminal networks are coopted or promoted by their specific knowledge and skills. Actors close one another may form clusters. On the other hand, the loose coupling of actors entails that if an actor or tie is ineffective, it can be removed or replaced. Participation in these networks is usually temporary and opportunistic, with only a few enduring actors providing continuity. In this way, individuals will drift in and out of the networks usually to perform a specific role (BRIGHT; MALM, 2019).

Moreover, the versatility of such criminal networks lets them rapidly adapt to changes in the environment and shift activities to exploit new opportunities. To enhance performance, networks may modify their existing structure by shifting their boundaries to either expand to gain access to new resources with low cost, add new individuals with the required skills, or contract to provide more security to its members and operations. Furthermore, their simple physical infrastructure allows them to easily relocate to other geographical locations to hinder law enforcement disruption (GERSPACHER; DUPONT, 2007; BRIGHT; MALM, 2019).

Given the unstable environment where illicit markets operate due to disruption, arrests, and seizures, network formation appears to the optimal social structure, providing more efficient communication, operations, and resource exchange, as well as adaptability to changing circumstances. In this sense, network resilience reveals how criminal networks can sustain endogenous and exogenous shocks to keep performing its primary activities and generate profit. Moreover, there is a need to balance maximizing efficiency and ensuring security, especially when it comes to performing a coordinated action. One way to increase security, for example,

is through redundancy, in which many actors perform the same role or tasks, and there is also a greater number of alternate social paths (BRIGHT; WHELAN, 2020).

In the light of the interconnectedness of criminal groups operating as networks and the challenge of untangling them, criminalists have been employing over the last two decades the methodology of Social Network Analysis (SNA). It allows to identify criminal network participants and clusters, map their relations and resources, and trace their financial flows and the interconnections between legitimate and illegitimate business. As a methodological and analytical tool, SNA enables, along with other criminological tools, to understand the structure, operations, strengths, and vulnerabilities of organized criminal networks (BRIGHT; WHELAN, 2020).

1.5.2 Security Networks

Taking stock of criminal networks and terrorism threats, governments and law enforcement[1] agencies, especially in the USA, Canada, EU, UK, and Australia, have adopted a network morphology as a new form of Security Governance. After the 9/11 terrorist attacks, the USA, for instance, has adopted networked modes of coordination, cooperation and collaboration with the creation of formal and informal linkages between public and private actors, such as the formation of Fusion Centers (WHELAN, 2017).

Security Governance is a concept that denotes the transformations of security policymaking, after the end of the Cold War, with the fragmentation of such policies among state and non-state actors, and the effects of their implementation. Scholars on the subject aim at identifying who dominates contemporary security governance arrangements and why, as well as the condition for effective and efficient functioning of new security arrangements, such as network modes of cooperation/collaboration of state and non-state actors in the form of Security Networks (KRAHMANN, 2005).

The concept of Security Network is used as metaphor by some authors to refer to pluralistic law enforcement arrangements. However, in this report, we take on a SNA perspective to Security Network, which refers to a set of institutional, organizational, or individual actors that are directly or indirectly connected in order to authorize and/or deliver security for the benefit of internal or external stakeholders. These actors, or nodes, are interconnected through different relational ties on a voluntary, contractual, or regulatory basis (DUPONT, 2006). In view of this definition, we adopt an Inter-Organizational Network

[1] Law Enforcement in this report refers to public and private organizations/agencies that deliver security.

approach to Security Networks as a form of governance, in which organizations/agencies represent security actors. As a form of governance, Security Networks allow participants to sustain, in the short- or long-terms, cooperation relationships, based on trust and reciprocity, which foster knowledge, information and intelligence sharing, better communication, and access to resources and capacity (BRIGHT; WHELAN, 2020). It is important to note here that while Security Networks may be involved in policy and regulation discussions, their main concern is the authorization and delivery of security through interactions, processes, and mobilization of the resources available, aiming at deploying human and technological assets, and managing risks (DUPONT, 2006).

As a form of networked governance, the concept of Security Networks is closely related to another concept, "Nodal Governance", which entails a pluralistic, decentralized view of security, eschewing the traditional dichotomy of public and private agents. Nodes are considered "providers" of governance, that is, organizations that harness and bring together ways of thinking and acting with an intent to shape the flow of events to promote their objectives. Nodal Governance conveys the idea that the different functions and organizational modes of law enforcement are understood as plural and heterogenic (HOLLEY; SHEARING, 2017). Security Network differ from the concept of Nodal Governance in a way that actors in a network not only work towards accomplishing their individual goals, but also the collective goal of the whole network, and for that they form relational ties with one another creating an interdependent environment.

The interactions and exchanges among actors in a security network are guided by the capacity to poll resources to increase effectiveness and decrease vulnerability. Hence, the advantage of this approach lies on the fact that security is seen not as the outcome of specific activities of each agency but as whole, that is, the product of many interactions and interdependencies among participants (DUPONT, 2006; WHELAN; DUPONT, 2017). Still, Dupont (2006) points out that the paradigm shift in security formations from hierarchies to networks has not been easily implemented, and sometimes shortfalls in effectiveness and success due to resistance from law enforcement actors. Security networks usually bring together a myriad of actors from different security organizations and law enforcement agencies with differing organizational cultures, procedures, and practices.

From an operational perspective, Security Networks are employed in diverse fields to solve a myriad of security problems. Table 13 shows the distribution of security issues in a comprehensive study of 117 security networks (WHELAN; DUPONT, 2017). In the study, the institutional configuration of the networks surveyed favoured hybrid relations between public,

private, and community stakeholders. We highlight (in yellow) in the table some “wicked” problems, with organized crime and drug control, which are the main concern of this report, appearing in 7 and 9 places, respectively

Table 13: Distribution of security issues (adapted from WHELAN and DUPONT, 2017)

Issue	**Number**	**%**
Urban security	46	39,32
Counterterrorism	16	13,68
General policing	13	11,11
Cybercrime	7	5,98
High policing	4	3,42
Transport	4	3,42
Organized crime	4	3,42
Mega event	4	3,42
Drug control	4	3,42
Police socialization	2	1,71
Campus security	2	1,71
Emergency management	2	1,71
Border security	2	1,71
Human trafficking	1	0,85
Resource extraction	1	0,85
Health	1	0,85
Rural security	1	0,85
Various	3	2,56
Total	117	100

To analyze and assess the complex and multidimensional nature of Security Networks, researchers make use of the theoretical-methodological toolbox of SNA to map actors, measure and analyze network relational structure properties, as presented earlier in this chapter. Researchers of Security Networks argue that a detailed knowledge of interactions that occur in the network can better inform security strategies and policies, and guide interventions at the operational level. For that, they also employ an Organizational perspective focusing on network types and functions, design, governance, and effectiveness, as discussed earlier. The next subsections summarize some key characteristics of Security Networks found in empirical research (WHELAN, 2012; 2017; WHELAN; DUPONT, 2017; BRIGHT; WHELAN, 2020; BREWER, 2012; 2017).

1.5.2.1 Dimensions, Types, and Functions

Literature on Security Networks identifies different dimensions of Security Networks: subnational, national, and transnational across de fields of High Policing and Low Policing[2]. Generally, Security Networks are goal-oriented, either mandated by government or by a lead agency appointed by government, but they can also arise from informal relations. Table 14 presents different features of Security Networks studied at the subnational, national, and transnational:

Table 14: Networks dimensions across the security field (adapted from WHELAN; DUPONT, 2017)

Network dimension	**Network goals**	**Network participants**	**Network ties**	**Network dynamics**
Subnational	Local crime and security problems within defined territorial or jurisdictional boundaries Networks are typically goal-oriented, but these goals may only be loosely stated.	Participation is usually open to public and private security agencies. Limited security classification constraints restricting participation.	Ties are usually physical as in structured meetings, with support of some virtual systems Informal ties play a prominent role due to physical and institutional proximity.	Leadership can shift between public and private actors, although local police will often adopt central positions. Relationships are largely shaped by individual participants on an interpersonal basis.
National	National crime and security problems, or those crossing intra-national borders. These include organized crime, drug trafficking, and terrorism. Networks are largely goal-oriented with articulated objectives and often outcome-focused.	Participation is usually limited to public security agencies, with private actors involved on the periphery on a case-by-case basis, mainly as a source of intelligence. Medium to high security classification constraints restrict participation and mode of operations.	Ties are both physical and virtual in nature, including structured meetings, liaisons, fusion centers, and intelligence databases.	Leadership can be a source of tension as security agencies often consider themselves to be equals and yield significant political influence. Relationships shaped by inter-organizational and interpersonal dynamics.

[2] Canadian criminologist Jean-Paul Brodeu (2007) distinguishes high policing from low policing. High policing involves the strategic use of intelligence; the conflation of separate state powers; the protection of national security; and the use of human resources and undercover operatives. Low policing refers to the maintenance of order and the general suppression of crime.

Transnational	Transnational crime and security problems or those crossing national borders. Networks are goal-oriented with articulated objectives and strict modes of governance.	Participation includes supranational and public security agencies with private actors involved on the periphery on a case-by- case basis, especially when they display unique forms of technical expertise. High security classification constraints and restrict participation and mode of operations	Ties are both physical and virtual, but more often facilitated by liaisons and information and communication systems.	Leadership can vary between lead-country or lead-organization depending on the nature of the task and network. Relationships shaped by international and inter-organizational dynamics.

As discussed earlier in this chapter, Inter-Organizational Networks have different types and functions (see table 4). Research points out four network types that have considerable relevance across the security filed, as shown in the table below:

Table 15: Network types across the security field (adapted from WHELAN; DUPONT, 2017)

Network type	**Network function**
Information exchange networks	Facilitate the sharing of information across intra- and inter-organizational boundaries. Examples include automated police systems and crime intelligence databases.
Knowledge-generating networks	Generate new knowledge (understood as processed information enabling decision-making) and distributes this knowledge between organizations. Examples can best be identified in relation to organized crime and terrorism threat assessments. Evidence-based policing networks that seek to identify and disseminate best-practices also belong to this category.
Problem-solving networks	Develop responses to complex or “wicked” problems that cannot be addressed by organizations acting alone. Examples include local security networks focusing on crime prevention initiatives to reduce gang violence or third-party policing interventions to improve quality of life.
Coordination networks	Coordinate joint responses and service delivery across organizational boundaries. Examples include joint police taskforces operating in the field of disaster and emergency management.

Each of the types shown in table 15 can be identified at the subnational, national, and transnational dimensions, with participants, nature of ties and processes varying in accordance to network’s specific goals and operational requirements. As with most typologies, there can

be an overlap between types, and it is important to note that networks can have multiple functions. For instance, a network can start with the primary goal of information sharing, while another network may use information sharing in order to solve a problem or coordinate roles and responsibilities among actors. Besides, there can be knowledge-generating networks existing as clusters of larger coordination networks.

Networks are created to tackle diverse security issues as seen in table 13. To deal with "wicked" problems, security networks are usually built on a temporary basis, short- or long term, with emphasis on gathering participants and resources across different professional and jurisdictional fields and even national borders. Examples in the field of organized crime include taskforces that are formed to perform a particular goal such as disrupt criminal activities in a particular space and time, or arrest and prosecute members of an organized criminal group. These "episodic" networks are usually of the problem-solving or coordination type. On the other hand, "enduring" networks are more on-going in nature without a pre-defined time, and they are more likely to be Information Sharing and Knowledge-Generating. Examples of these type are Fusion Centers and threat-assessment centers. Fusion Centers are formal networks configurations, first established in the USA and latter in other countries such as Australia. Fusion Centers work as "coordinating hubs" across the USA for the collection, analysis, and dissemination of national security intelligence among federal, state, and local law enforcement agencies and related stakeholders.

1.5.2.2 Design – the structural relations

When designing a Security Network, especially a goal-oriented one, the first consideration should be selecting the agencies that have a stake on the goal of the network and can meaningfully contribute to this goal. Usually, a leading or founding agency/organization is appointed to articulate the network goal(s) and recruit the participants.

Unless mandated from the beginning, the formation of network ties is a two-way process and requires that an agency be motivated to join the network (usually when the individual goals of the agency align with network goal) and that other networks members see the value of the agency joining in. Researchers call attention to including more agencies in a network, which is not always effective. Ideally, there should be enough diversity for a network to have complementary expertise with few redundant ties.

The preferred network structure and the amount of integration in a network depends on a number of factors including purpose, size, type and function, governance, and mode of

operation. Most of the times there is no need to integrate all actors in a dense set of relationships in the network. Organizational network scholars advocate for a more selective integration, in which network ties are targeted and appropriate to create more dense ties among agencies that need to work closely together, while others do not. In this way, selective integration calibrates density and centralization in a network. For instance, if density and integration are too high, it is likely that the network will be inefficient due to too much redundant exchanges, such as generating too much redundant information. A solution is to centralize the network around a lead agency in a way that agencies can communicate through it, facilitating coordination and cooperation (PROVAN; LEMAIRE, 2012).

Considering the network theoretical approaches of Structural Hole and Closure, discussed earlier in this chapter, network designs should make use of strong and weak ties, maximizing close and strong ties among agencies with more aligned goals in the network, while creating bridges and brokering opportunities in distant and weak ties, optimizing exchanges such as novel information from clusters or peripheric actors. Research on Security Networks shows the need for a network to be fairly stable at its core, while maintain flexibility at its periphery. The network core should consist of agencies that are central to network goals, while flexibility is advantageous for agencies less connected and whose involvement is less crucial. In this way, new agencies can enter bringing new ideas and resources to core members, while less involved agencies can leave.

1.5.2.3 Governance, Management and Effectiveness

As seen in previous section 1.4.2 of this chapter, there are three ideal types of Inter-Organizational Networks governance and important contingencies that play a role in network effectiveness. In the security field, networks less structured are more likely to have Shared Governance, while very few will be governed by a NAO. Knowledge-Generating networks usually varies in network governance based on the specific purposes of each network, usually most will also involve a Lead Organization. Fusion Centers are examples of networks governed by a lead agency. Some Information-Sharing networks work automatically with the aid of intelligence-sharing databases and systems based on protocols guiding their governance. In this context, when new intelligence is uploaded in the system, it is automatically disseminated to network members. In such networks, there is a need to balance information protection with information sharing. Usually that requires some policy framework or agreement to exchange classified information, together with protocols to ensure data is protected from cyber-attacks.

Regarding law enforcement responses to organized crime, most Security Networks are brokered by a Lead Organization that assumes a central position in the network. This is particularly important in problem-solving and coordination networks where strong leadership is key to achieving network goals. Usually, these networks will have some kind of management or steering committee, which gathers representations from the lead agency and other agencies comprising the core of the network. A strategic purpose of these committees is to establish priorities for the network and manage conflicting goals and organizational cultures.

It is known that networks are not efficient and effective from the start. Researchers call attention to the need to balance the structure of the network with flexibility, so the process and relationships within the network can develop and evolve more organically. Relationships take time to develop especially cooperation ties based on trust and reciprocity, as discussed earlier in this chapter. Besides, there is the tension between inclusiveness and efficiency in the sense that the more participants are involved in the network, the more time consuming and resource intensive (and hence less efficient) that process tends to be.

To develop more sustainable and effective Security Networks, some factors are highlighted: Trust; Value and Goal Consensus; Organizational Culture; and Management of Power Imbalances. Empirical research in the context of law enforcement responses to organized crime show that these factors are intrinsically connected. For example, the more shared goals and stronger the relationships based on trust, the more the actors will cooperate to ensure the success of the network.

Trust

As seen in earlier in this chapter, trust is crucial in creating strong relationships that encourage cooperation among network actors. In Security Networks, representatives of organizations usually distinguish personal trust from organizational trust, but recognize that they are intrinsically linked, that is, interpersonal and inter-organizational trust are central to network cooperation and operations. There are five key challenges related to initiating and sustaining trust that are consistent with empirical research on Security Networks: forming expectations; managing risk; managing dynamics; managing power imbalances; and nurturing collaborative/cooperative relationships (HUXHAM; VANGEN, 2005, p. 172 *apud* WHELAN; BRIGHT, 2020). Besides, trusting relationships help build network Social Capital, which in turn enhances network effectiveness by way of fostering cooperation. The results of a study (BREWER, 2012) conducted on American and Australian waterfronts revealed that cooperation relies on trust, and when lacking cooperation is inhibited.

Value and Goal Consensus

It is essential for networks to be recognized as entities that create value for its participants, its internal and external stakeholders, and the community. However, disagreements may arise when network outcomes or results conflict with an agency's independent mandate or objective. Regarding goal consensus, it is desirable that network goals align with actors' individual goals, which can be maximized when all actors have a say in the goals of the network. This also involves the creation of shared goals to promote cooperation. In some networks, though, diversity plays an important role, such as in Knowledge-Sharing networks, in reducing the likelihood of "group thinking". One should note yet that shared goals and individual goals can change overtime, which might create conflict among network participants.

Organizational Culture

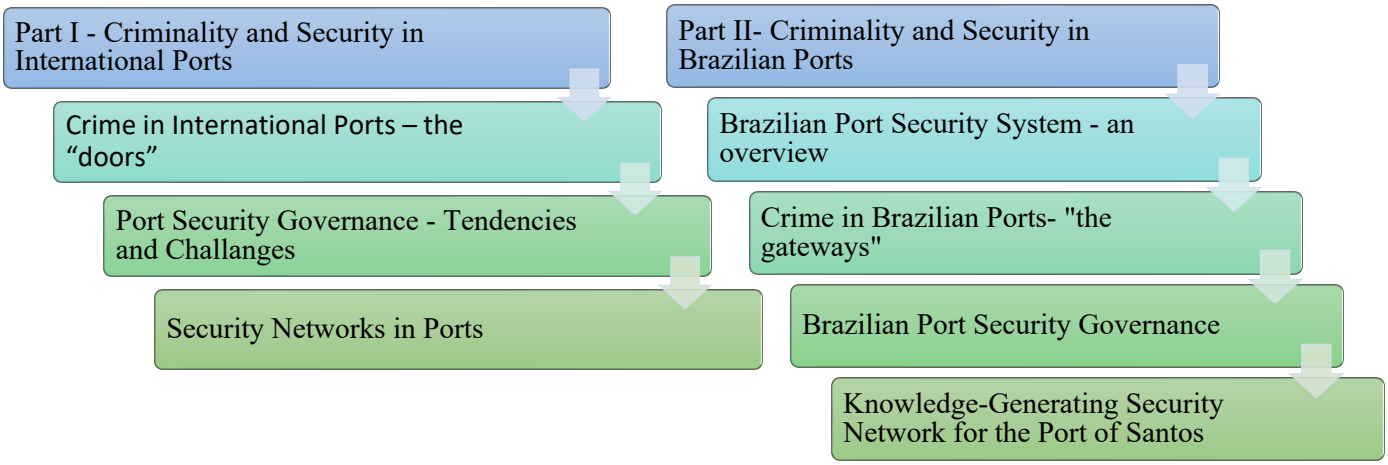
When joining a network, organizations usually bring their own organizational cultures, which involve different mentalities, practices, and processes. Differing cultures can pose a challenge to actors' agreement on network shared goals, strategies, processes, and outcomes. It can also hamper communication in the absence of a common language. Research shows that organizational culture develops by means of dynamic relational processes and has the potential to change, as actors in a network interact with one another. In this context, different organizational cultures shape the network, and the network may shape organizational cultures as well. There are some intentional mechanisms for changing culture, which include strategies to promote interagency cooperation through shared goals, as well as efforts of central actors in a broker position to merge or moderate cultural differences.

Management of Power imbalances

Ideally, in a network, power is dispersed in horizontal and interdependent relationships. Actors cannot simply assert their authority but must negotiate its terms. In this sense, an independent decision from one agency can have a ripple effect on the network, having consequences for its participants. Power imbalances in a network entail actors with sources of power, such as formal authority, occupying central positions, or having privileged access to tangible and intangible resources, which might influence the design, purpose, and operation of the network. Moreover, agencies residing at the periphery of the network may have limited participation, since they occupy more passive positions either by choice or constrain in some way.

Chapter 2: Port Criminality and Security Governance

Roadmap to chapter



Part I – Criminality and Security in International Ports

2.1 Crime in International Ports – the "doors"

Research empirical data on port criminality (SERGI et al., 2021; SERGI 2020a; 2020b; 2020c; ANTONELLI 2020; ROKS et al. 2020) collected in the ports of Genoa and Gioia Tauro, in Italy, Rotterdam, in the Netherlands, and Antwerp, in Belgium, reveal the complex nature of organized crime and its many illicit activities in and around ports. In almost all major European seaports, organized crime usually takes on networked and transnational aspect, with crimes ranging from drugs and arms trafficking, smuggling of counterfeit goods and other illicit trade, human trafficking, to infiltration and interference in the port economy and governance, as well as corruption of port operators and other personnel. Criminals exploit the logistics infrastructure and supply chain of ports to carry out their illicit activities. Ports are also strategic spaces where criminal networks can expand social ties and carry out illegal (and sometimes legal) businesses.

Blue Crimes

Criminality that takes place ports is considered by researchers of Maritime Security a type of "Blue Crime" (BUERGER; EDMUNDS, 2020). Crimes at sea, or "blue crimes", have different expressions across maritime regions, affecting shipping, international trade, economic interests, and even national security. TOC has become an important threat to Maritime Security with crimes ranging from piracy, illicit trade of goods, drugs, weapons, and human trafficking, to environmental crimes, such as pollution and illegal fishing. (BUERGER; EDMUNDS, 2020).

Port criminality correlated with the illicit market maritime routes. Drug trafficking routes are found along usual international trade routes, and criminal networks are constantly seeking methods and paths that facilitate the use of existing transport modes (land, water, and air). Criminal networks are also very resilient and adaptive with the capacity to diversify routes to changing circumstances and law enforcement disruption. Almost 90% of cocaine seized by authorities worldwide is linked to maritime trafficking. International drug traffickers make use of different sea routes to transport cocaine produced in the Andean countries of Colombia, Peru, and Bolivia to consumer markets in Europe, USA, Africa, and Asia (UNODC, 2022). Figure 6 shows the main global cocaine routes, and figures 7 and 8 show the countries that are source, transit, and destination of cocaine shipments.

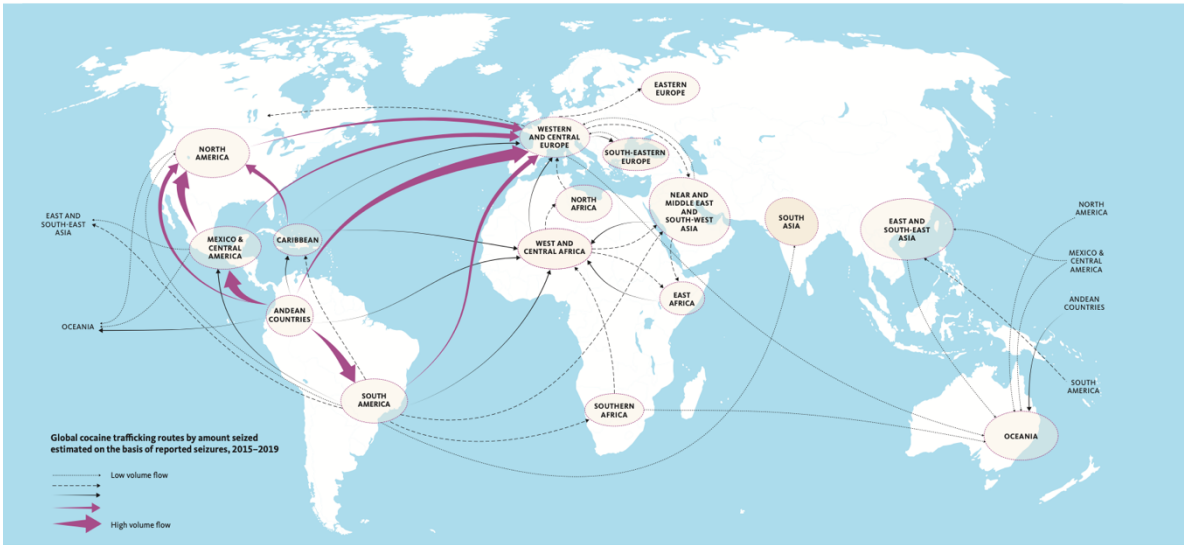


Figure 7: Global cocaine trafficking routes by number of reported seizures 2015-2019 (UNODC, 2022).

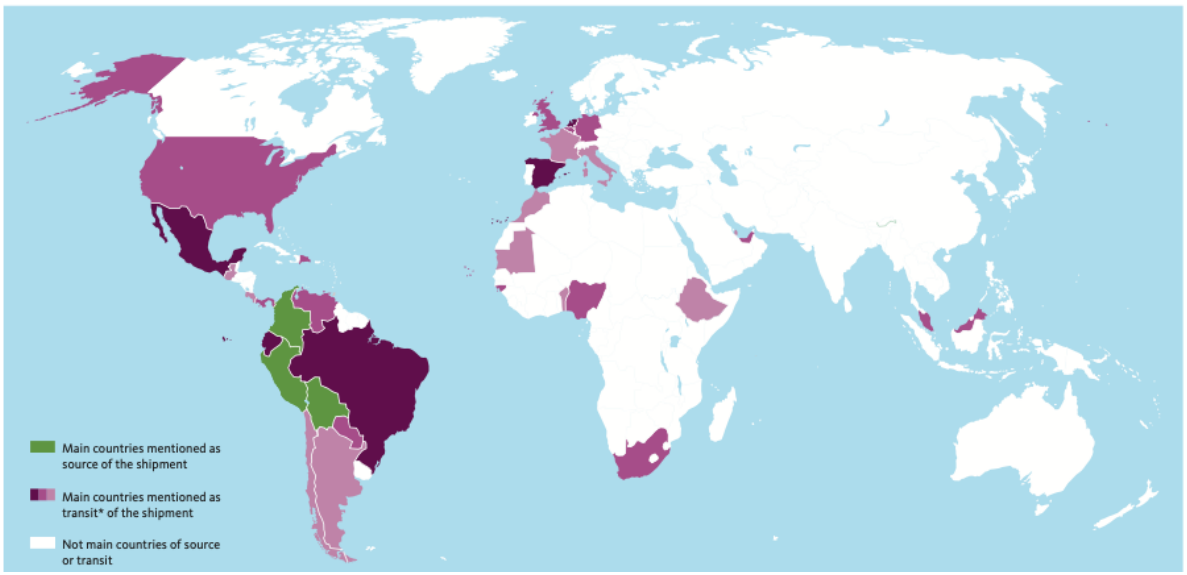


Figure 8: In green, countries reported as source of cocaine shipment. In purple shades, countries reported as transit of shipment (UNODC, 2022).

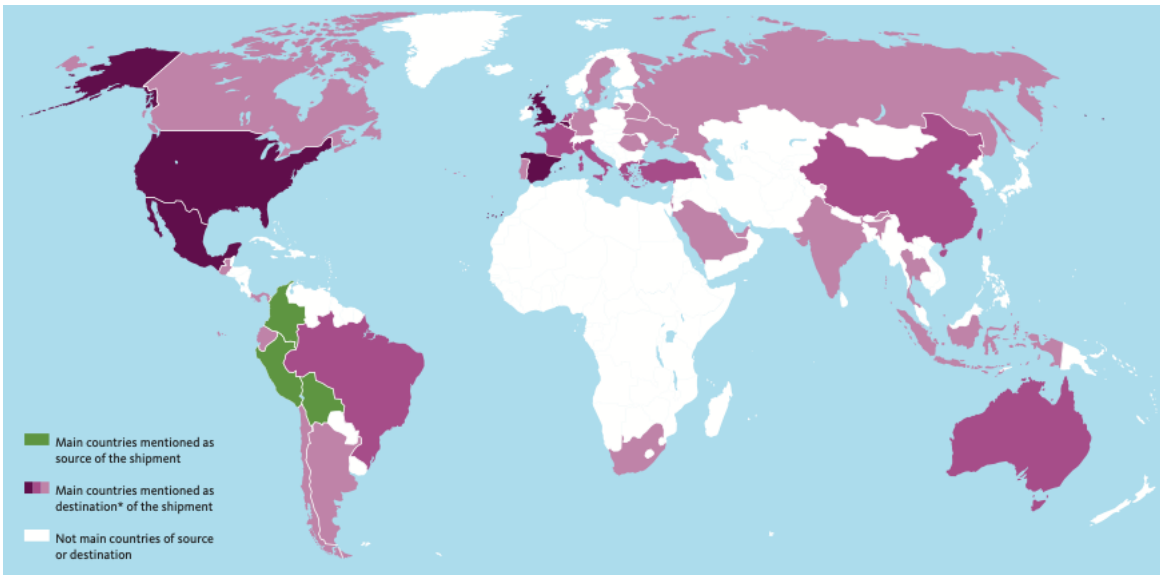


Figure 9: In green, countries reported as source of cocaine shipment. In purple shades, countries reported as destination of shipment (UNODC, 2022).

The cocaine trafficking sea route between South America and Europe is nowadays one of the major routes of international drug trafficking. In this scenario, seaports in South America, such as the Port of Santos, the largest and busiest in the region, are important "gateways" for TOC to transport cocaine to consumer markets in Europe. The illegal cargo arrives in the continent by its largest ports, or "doors", such as those of Antwerp, Rotterdam, Genoa, and Gioia Tauro (UNODC, 2022). The shipment is usually received by criminal and mafia type networks acting around the port-city area to be latter distributed to its consumer markets in European cities (SERGI et al., 2021).

It is known that European criminal groups, such as "Ndrangheta", one of Italy's largest and most dangerous mafia groups from Calabria, have established cooperating and business ties with other criminal groups in the Andean countries and with Brazil's largest criminal group "First Command of the Capital" (PCC). Besides, there are new criminal actors among transatlantic cocaine traffickers, which include organized criminal networks from South-Eastern Europe orchestrating the trafficking of significant amounts of cocaine to Europe. Cocaine shipment from South America is also entering Europe through West and Central Africa and North Africa (UNODC, 2021).

Traffickers are very creative in hiding the drugs and bypassing port surveillance and control checks, in a "game of cat and mouse" with port security providers. Criminals use several "methods" to hide drugs onboard ships and/or containers. The most common practice is the "rip-on rip-off" method, in which criminals attempt to conceal drugs in containers which have

already undergone checks carried out by customs officials. The drugs are hidden in different types of cargo, ranging from commodities to electronical and machinery. They also hide drugs inside several spots inside ships like the anchor, funnel, water inlets, fuel tanks, and in the hull and vents. For underwater spots, criminals usually hire professional divers to carry out the task. In other cases, they may employ the "fishing" method, in which a smaller vessel carrying drugs approach the ship where coopeted sailors are waiting to hoist the illegal cargo on board.

Empirical research on European ports (SERGI et al., 2021) show that criminal networks are sometimes embedded in the ports' infrastructure, taking advantage of the legal flow of goods to create space and opportunities for their illegal (and legal) activities. Criminals engaging in such activities benefit from social relations, since there is always a port employee or operator willing to work as a "trusted insider" providing information on import and export practices conducted in port facilities. Criminals also obtain knowledge about the port's logistics processes, supply chain, and security measures to successfully make use of terminals, containers, vessels, and other port facilities to carry out their activities undetected. They often copy names and addresses of companies with good reputation to export and import as legitimate suppliers, making use of the "green lines", that is, avoiding extra checks. Besides, port economy usually intersects with the city/region economy and social space, thus creating opportunities for corruption and infiltration in public and private contracts, in or around the port area, which might disrupt the governance of port administration, for instance. Usually, organized crime infiltration or attempt to infiltrate port economy and administration is discovered during law enforcement operations to counter drug trafficking, for example (SERGI, 2020b).

Criminal networks also carry out a variety of cybercrimes, since ports nowadays rely heavily in technologies to control and enhance port administrative governance and security. Port employees with access to these technologies can become targets of criminals that seek to coopt them. Besides, the increased reliance on technologies can create systemic vulnerabilities to which cybercriminals can take advantage of. For example, hackers may seek to gain access remotely to information on cargo or shipments or to blackmail or extort port operators (SERGI et al., 2021).

2.2 Port Security Governance - Tendencies and Challenges

Given the diversity of illicit activities carried out by organized crime in the waterfront, port security requires specialized and diversified law enforcement approaches, from hybrid policing, joint task forces[3], to partnerships and security networks at the local, national, and transnational levels. The concept of hybrid policing is understood not as the sum of many security agencies' activities (including private security companies), but as the co-existence of many aims, which results in a constant tension between the local and global dimensions of port security. On one side, it is matter of national security and boarder control, and on the other, there is territorial everyday policing of port facilities and port-city areas. In this sense, port security involves a hybrid between high, intelligence-led policing and low policing (SERGI et al., 2021).

Case examples of policing illicit trafficking in ports, such as seizure of cocaine cargo, show that it generally requires national or transnational cooperation and coordinated efforts by port authorities and law enforcement agencies, including border customs and special port teams of municipal and federal police forces, and sometimes private actors. For example, investigations on cocaine trafficking may start in one country or region where criminals use ports as "gateways" to overseas markets and finish in another country or region where ports are used as "doors" to receive the illicit cargo, such as in the case of the South American-Europe overseas route, as seen in the previous section. Besides, since the opening of containers, where illicit drugs are usually hidden, is a difficult task due to increased border controls and to avoid disturbance in trade business, there is a need for law enforcement investigations to involve sometimes the whole transport system or supply chain, and in some cases to investigate instances of corruption and collusion of terminal personnel (SERGI et al., 2021). One example of international cooperation and coordinated effort is the UNODC-WCO Container Control Programme (CCP), which has greatly helped countries around the globe to build capacity, improve risk management, and secure supply chain by preventing the cross-border movement of illicit goods and drugs hidden inside containers.

The ISPS Code (International Ship and Port Facility Security Code), chapter XI-2 of the SOLAS Convention (The International Convention for the Safety of Life at Sea), is today the most important cornerstone guiding port authorities and law enforcement on security procedures and protocols. The ISPS Code is a vital part of the international maritime regulatory

[3] Joint task forces involve three or more security agencies working in a coordinated manner or in cooperation to achieve a common goal.

regime established after the 9/11 terrorist attacks. It is a comprehensive mandatory security regime for international shipping and port facilities divided into two parts. Part A details the mandatory maritime and port security-related requirements that SOLAS contracting governments, port authorities, and shipping companies must adhere to comply with the Code. Part B provides a series of recommendations and guidelines on how to meet the provisions outlined in Part A. The ISPS Code was developed to protect ports as critical infrastructure from the physical threats of non-state terrorist actors. Part A establishes formal responsibilities across port's public and private actors, such as nomination of the Port Facility Security Officer (PFSO), and it forms the baseline for cooperative activities and port security, which are mostly carried out through risk assessment and modeling, development of the Port Facility Security Plans, and personnel training (IMO, 2003).

Port security plans are tailored considering the geographical location of the port, flows arriving and departing, shipping routes, and criminal scenario across port facilities and port-city areas. In addition, security in most major international ports is based on situational crime prevention techniques, such as counter-trafficking efforts, which aim at monitoring, controlling, and banning access using surveillance and control techniques, including cameras with embedded AI (Artificial Intelligence), scanners, smart cards, physical barriers, and so on (SERGI, 2020b). In this context, technology advancements and cybersecurity play a crucial role in enhancing security in port environment and terminals, as well as improving communication and information sharing through integrated systems and databases. The concept of "smart ports" entails ports that aim to achieve an integrated, fully digitalized, and completely traceable end-to-end supply chain in the port and its hinterland, by making use of advanced technologies such as IoT (Internet of Things), VR (Virtual Reality), BIM (Building Information Modeling), AI, and Big Data.

Considering the ISPS Code mandatory measures and recommendations and to increase port security efficiency and effectiveness, port authorities and law enforcement, especially in Europe, USA, and Australia, have encouraged interagency approaches to port security, especially regarding private and public partnerships, joint task forces, or networks to tackle the complex criminality in ports. Cooperation fostered by security networks, for instance, is beneficial for security stakeholders in a multifaceted and vast environment such as ports. Moreover, law enforcement operations are more effective and efficient when in coordination with the private sector, for example, which has access to important data needed to prevent and disrupt criminal activities in port facilities (POMERLEAU, 2019).

Information sharing is a crucial component for cooperation in networks and coordinated operations. It includes different technology platforms and databases, and in the case of networks, it also involves interpersonal and inter-organizational relations as well. Research in major European ports (SERGI et al., 2021; SERGI, 2020b) show that law enforcement agencies and other public agencies operating in port security struggle to establish consistent communication and information channels with private companies and their security actors and vice-versa. This is due to the following challenges (SERGI et al., 2021, p. 12 -13):

- Cooperation problems: different and competing priorities for agencies and organizations active in policing and securing the waterfront, often working in siloed manners. This also includes conflicting work mentalities due to diverse organizational cultures.
- Coordination problems: overlapping jurisdictions, mandates, and duplication of effort in approaching certain investigations/security issues. Besides, each security agency usually has their own work protocols, processes, and practices.
- Privacy concerns: inconsistent or incompatible confidentiality protocols, data sharing cultures, and requirements.

Taking such issues into consideration, most cooperation and coordinated operations take place in an *ad-hoc* basis, such as in joint task forces to seize illegal cargo, carry out arrest warrants, or when intelligence-led investigations need support or access to port facilities and/or other organizations working within the waterfront. However, according to Sergi et al. (2021), *ad hoc* approaches tend to be unsustainable or ineffective in the long run. Most intelligence-led policing and risk-based approaches usually rely on consistent information and data sharing to detect systematic breaches and to improve overall port security governance. Besides, drug trafficking, as a truly transnational problem, requires permanent cooperation among security agencies and concerted intelligence-led and cross-border efforts. In the next section, we will discuss in more detail how security networks can help foster and strengthen more long-term cooperation and more efficient and effective coordination efforts.

Another issue found by empirical research that puts pressure on cooperation and operational coordination across port security providers is the effect of privatization in port environment, economy, and governance. Research (SERGI et al., 2021; SERGI, 2020b; NOKLEBERG, 2019) shows that the public and private dichotomy creates relationship tensions among actors in an already complex setting, which can have negative effect on information sharing, cooperation, and the overall effectiveness in delivering security.

When observed as territory, port governance is usually divided among public and private stakeholders. In this environment, relationships between private terminals and public

authorities are sometimes known to be confrontational, especially regarding port security due to different objectives and priorities. While private terminals aim at improving operations and productivity, public law enforcement aims at crime prevention and disruption. Examining this relation in the port of Genoa, Italy, Sergi (2020b) observed that the relationship among these actors is amicable, however private companies, as "tenants" of port facilities, see public law enforcement entering their premises as something troublesome to their daily activities and as an "intrusion" into their territory. This "tenant mentality" results in lack of public and private engagement, which can limit law enforcement knowledge on private terminal's processes and systems, hampering investigations on corrupted personnel, such as "trusted insiders", and their activities, for example.

In most major ports carrying overseas trade, there is another inherent tension: trade facilitation versus security. Privatization of port economy prioritizes privacy and smooth business transactions. Because of this, law enforcement and customs agencies have difficulty in accessing private port premises without interrupting business. Furthermore, business that employ private security teams sometimes have divergent priorities and targets. These private security actors, although willing to cooperate with authorities, may face incentives, explicit or implicit, to prioritize the continuity of business, for instance. However, there is a growing awareness among port stakeholders that security issues may have economic consequences, particularly regarding reputation. But for these stakeholders, to view security as an "added value" requires "added costs". From the point of view of law enforcement, though, trade and security are mutually reinforcing (SERGI, 2020b).

When it comes to security breaches due to corruption, research shows that law enforcement usually lacks the resources needed to detect and deter systemic corruption. For example, law enforcement is more efficient in detecting and tracing corruption when actions are coordinated with the private sector, which has access to a vast quantity of data needed. Also, private sector professionals' skills in cybersecurity and data analytics could be used to leverage the knowledge and legal power of public authorities in this matter (SERGI et al. 2021; POMERLEAU, 2019).

Finally, port researchers and practitioners argue that international maritime and port security regimes mostly focus on the port-sea interface through maritime protocols, with little attention given to the port-city interface. To tackle drug trafficking, for instance, it is vital to understand the impact of criminal groups operating in the port-city areas, and their criminal investments, usually undertaken by money laundering. The current instruments of maritime security do not always provide the right mandate to allow law enforcement to investigate and

prosecute criminality at sea and ports. Such instruments also do not consider the need for hybrid policing to deliver security in the multidimensional and multifaced infrastructure of ports. Furthermore, critics of the ISPS Code state the need to adapt it, together with the introduction of new international codes and protocols, to better represent the reality and modus operandi of crime in ports, especially criminal networks involved in drug trafficking (SERGI et al., 2021).

2.2.1 Port Security Networks

Given the hybrid, multi-organizational aspect of seaports, empirical research on port security reveals that practitioners are overwhelmed by the number of actors who play a role in the security provision in the port environment, making it difficult to identify potential partners or developed relationships at the local, national, and transnational levels (SERGI et al., 2021). In this light, scholars in the fields of Criminality and Security Studies argue that the network perspective can be a useful framework to describe the complexities of security governance in ports. In special, the theoretical and methodological tools of SNA can be an important tool to map actors and their formal and informal ties in the multifaceted port environment to provide a clearer picture of the socio-structure of security providers (BREWER, 2017).

So far, regarding research on port criminality and security governance, there have been only a few empirical studies on port's security networks. The lack of research in this area is mostly due to researchers' difficulty in finding and engaging security organizations representatives (both public and private) that are willing to share their work experience and relations with other security providers. The reason behind this is usually security organizations' confidentiality and privacy concerns and other individual issues.

We highlight in this report three empirical researches on port security networks: Dinchel and Easton (2021 *apud* SERGI et al., 2021), Eski (2016), and Brewer (2012). We point here that in Dinchel and Easton's (2021) and Eski's (2016) studies, the concept of Security Network is used as a metaphor to explain and map the changes and pluralization of security governance in ports. Brewer (2012)'s study, on the other hand, employs the theoretical and methodological tools of SNA and the Inter-organizational Network perspective (discussed in the first chapter of this report) to analyze the security networks of American and Australian ports. Moreover, each research employed other research methodologies, such as case study, ethnography, semi-structured interviews, surveys, and so on.

Building on multi-sited ethnographic fieldwork in two major European ports, Eski's (2016) research discussed how operational policing and security realities and identities are

established and examined how industrial commercialization has aggravated security issues. The study portrayed a compelling empirically balanced account of the attitudes and practices of port police and security officers, by focusing on issues such as port security management and governance, multi-agency policing, and port complex crimes encompassing drug trafficking, human smuggling, and terrorism.

Brewer's (2012) research on the security networks of the ports of Los Angeles, USA, and Melbourne, Australia, called attention to the fact that Social Capital is rarely explored in empirical studies in the field of Criminality and Security. However, the concept has much to reveal about the nature of relationships between public authorities and private actors, and the potential for cooperation to achieve more successful outcomes. For that, the scholar employed SNA tools to map the social structure of security providers in both ports and its formal and informal relations among public and private actors. The research showed that actors in the security network of the Los Angeles Port can mobilize their highly connected network, place trust in their peers, fostering meaningful engagement resulting in co-production activities. These features indicate that Social Capital created and made available in the network is a surplus, which is advantageous for overall network performance. On the other hand, in the security network of Melbourne Port, Social Capital is hampered by conflicting perspectives that contributed to a lack of trust among network actors, hindering engagement aimed at co-production activities. Brewer concluded that trust plays an important role in developing strong, effective and efficient security networks engaged in cooperation efforts to control crime in the waterfront. Moreover, the research highlighted that private actors in broker positions in the networks act as conduits of exchange (information and resources) and can build trust and bridge otherwise disconnected actors.

In Dinchel and Easton's (2021 *apud* SERGI et al., 2021) research on security governance of the Port of Antwerp, representatives from organizations such as police forces, customs, port authority, terminal operators, private security companies, and other private actors reported to regularly participate in over 30 different security configurations (networks, partnerships, or taskforces) dealing with port security and also maritime security on the local, regional, national and transnational levels, as well as in information virtual networks. The research found that although transnational networks are crucial to improving port and maritime security, practitioners reported participating more in local and national security configurations given more immediate concerns. Besides, the high workload and lack of time hindered building relationships with other counterparts in foreign ports. Practitioners reported the difficulty in finding the appropriate partners, since organization competences, such as the ones of police

forces and customs, vary from one country to another. The researcher also highlighted the "Stroomplan", a policy plan created to counter drug trafficking in the Port of Antwerp, which gathers several security actors and stimulates networking between them, while engaging them operationally and in cooperative endeavors.

Overall, according to Sergi et al. (2021), practitioners in European ports understand the importance of cooperating with law enforcement agencies at the local, national, and transnational levels. For instance, they have already acknowledged the importance of cooperating with law enforcement agencies in South America's cocaine manufacturing countries, and particularly in transit countries such as Brazil. Nonetheless, partitioners understand that cooperation efforts, even at the domestic level, rely on trust and reciprocity and can be inhibited by different mindsets and organizational cultures, which often creates tension and undermines integrated approaches. This also involves the "tenant mentality", discussed earlier in this chapter, which creates a divide between private and public actors. Furthermore, building cooperative relationships takes time and usually requires extra or special budgets, not to mention the development of new policies in the case of mandated networks. Below, a table summarizing the tendencies and challenges discussed in this section of the report.

Table 16: Tendencies and Challenges of International Port Security

Tendencies
ISPS Code Hybrid Policing – High and Low Policing Interagency coordination and cooperation (usually *ad hoc*) Security Networks Global Cooperation Programs (ex UNODC-CPP) Technology advancements and cybersecurity – "Smart Ports"
Challenges
Multifaceted environment – myriad of actors participating in port security governance Information sharing - cooperation and coordination problems and privacy concerns Public and Private divide in port environment – "Tennent mentality" Security versus Trade tensions Maritime and Security Regimes (including ISPS Code) limitations to tackle organized crime

Part II – Criminality and Security in Brazilian Ports

2.3 The Brazilian Port Security System – An Overview

Brazil has a maritime frontier of 7.491 km, with a high population density (58% of the total population), concentrating 95% of its foreign trade. For this reason, Brazil's seaports are a vital part of the country's economy and central hubs for transportation and the supply chain. There are 37 public ports in the country, managed by the Federal Government through Port Authority companies or under delegation agreement to states or municipalities, encompassing 168 private use terminals and 28 small scale cargo transshipment stations along the country's inland waterways system. According to the National Waterway Transportation Agency (ANTAQ, 2022), Brazilian ports and terminals handled 1.210 billion tons of cargo in 2021. The three main ports in the country regarding handling (t) are the Port of Santos, Port of Itaguaí, and Port of Paranaguá.

The Blue Amazon

As critical infrastructure, ports are part of the country's "Amazônia Azul" [Blue Amazon], a concept coined by the Brazilian Navy (MB) to raise awareness on the strategic importance and richness of Brazilian coastal areas, jurisdictional waters, and EEZ (Exclusive Economic Zone).

The Port of Santos, located in São Paulo estate, is the largest multipurpose port in Latin America, with a total of 53 terminals (including 6 private terminals). The port occupies an area of 16 km with total floor area of 7,8 mil of m^2 and is served by a complete and integrated road, railway, and pipeline transportation network. The top one port in Brazil regarding handling of containers and dry bulk, the Port of Santos is responsible for 28% of the country's foreign trade. The port is the main "door" and "gateway" of goods in Brazil, connecting more than 600 destinations in more than 200 countries (SANTOS PORT AUTHORITY, 2022).

As a member of IMO (International Maritime Organization) and a signatory of the SOLAS Convention, Brazil complies with the current security regime for International Ship and Port Facility Security Code (ISPS Code), which entered into force in July in 2004, in

accordance with the recommendations and provisions of IMO. Regarding the internalization of ISPS Code, it was approved by the country's legislators in 2009 (Decree-law No. 645 of September 18, 2009) and enacted in 2019 (Decree-law No. 9988 of August 26, 2019) (BRASIL, 2020). The implementation of the ISPS Code by the Brazilian government is divided between the Brazilian Navy (MP) and CONPORTOS (National Commission for Public Security of Ports, Terminals, and Waterways) (BRASIL, 2020).

The Brazilian Navy is the country's Maritime Authority represented by the Navy Command by way of the Directorate of Ports and Coasts. It provides safety and security for waterway traffic in the country's jurisdictional waters to safeguard human life, shipping safety in open seas and internal waterways, prevent environmental pollution, and it also regulates the country's merchant navy. Moreover, the Navy Command is responsible for accessing and approving the security plans of ships with Brazilian flags regarding the ISPS Code provisions.

The ISPS Code is internalized in Brazil's public ports and port facilities by way of CONPORTOS, which is a collegiate body comprised of representatives from the Ministry of Justice and Public Security (MJSP), by way of the Federal Police, which presides; the Ministry of Defense (MD), by way of the Brazilian Navy Command (MB); the Ministry of Foreign Relations (MRE); the Ministry of Economy (ME), by way of the Brazilian Federal Revenue (RFB); Ministry of Infrastructure (MI); and the National Waterway Transport Agency (ANTAQ).

The Resolution No. 53, of September 4, 2020, (BRASIL, 2020) which is currently into force, details the provisions of CONPORTOS based on the ISPS Code. The document specifies the attributions and responsibilities of CESPORTOS (State Commissions for Public Security of Ports, Terminals, and Waterways), as well as Port Facility Security Officers (PFSOs) and Private Security Organizations accredited by CESPORTOS to elaborate Port Risk Assessments and Port Facility Security Plans. Port risk analysis is carried out through the ARESP (Análise de Riscos com ênfase em Segurança Portuária) method (ALBUQUERQUE; ANDRADE, 2019), which guides the development of plans and procedures to address real or potential threats to port facilities that may have an impact on port activities. The Resolution No. 53 also regulates the programmed audits and inspections conducted in port facilities by CESPORTOS and CONPORTOS, and the Declaration of Protection and the Declaration of Compliance, in accordance with the ISPS Code, as well as other provisions, definitions, and annexes.

Subordinated to CONPORTOS and located in regions with international shipping ports, CESPORTOS are permanent collegiate bodies, which gathers representatives from the following agencies: the Federal Police (PF), which presides the commission; Captain of the

Port (MB); Brazilian Federal Revenue Office (RFB); National Waterway Transport Agency (ANTAQ); Port Authority Security Units; and Public Security Secretariat of State Governments. CESPORTOS attributions include approving Port Risk Assessments and Port Facility Security Plans, carry out inspections and audits in port facilities, conduct process analysis on the work of Port Facility Security Officers (PFSO) and Private Security Organizations, and execute CONPORTOS actions in States under their direct supervision (BRASIL, 2020).

The National Plan for Port Public Security, approved by CONPORTOS in 2002, but which is no longer into force, see that CONPORTOS also develops and implements the system for illicit acts prevention and repression in ports, terminals, and waterways, by way of resolutions and deliberations, which are carried out by CESPORTOS regional branches. It is an action plan aimed at improving public security in ports, terminals, and waterways considering the challenges of such complex environments, which gathers different governmental agencies, private entities, and civil society. The plan sets integrated measures to enhance the work of public security through the cooperation lenses. It states that only through joint participation, the program will be effective and will create an environment for more efficient and effective actions. The document also states the attributions and responsibilities of each port security actor (BRASIL, 2002).

2.4 Criminality in Brazilian Ports – The “gateways”

The dynamics of criminally in Brazilian major seaports is similar to the complex crimes found in international ports discussed in part I of this chapter. Crimes range from trafficking of drugs and firearms, smuggling of counterfeit goods and other merchandise, to corruption of port personnel. A recent assessment by the Brazilian Federal Court of Accounts (TCU) shows that the trafficking of cocaine is the main crime committed in port facilities, given the significant rise in drug apprehension by law enforcement over the last years (TCU, 2021).

Due to its extensive land and maritime borders, Brazil occupies a strategic position in the “geopolitics of cocaine”, as transit route (see figure 8) for cocaine manufactured in the Andean countries destined mainly to Europe, Africa, and Asia (UNODC, 2022). Brazil shares borders with Colombia, Peru and Bolivia, the biggest producers of cocaine in the world. It also shares boarder with Paraguay, which is a well-known hub, called the “Narcosur”, for transnational criminal networks, and the biggest producer of marijuana in South America. Drug cargos enter Brazilian territory through different land routes, as well as through air and internal

waters, where some of them end up in the country's seaports. Figure 10 shows the main trafficking routes in Brazil. In the map, one can see the connection between the areas of cocaine production, its transportation routes (blue lines), and export platforms (in purple), which include some of Brazil's major seaports (COE BRAZIL, 2021).

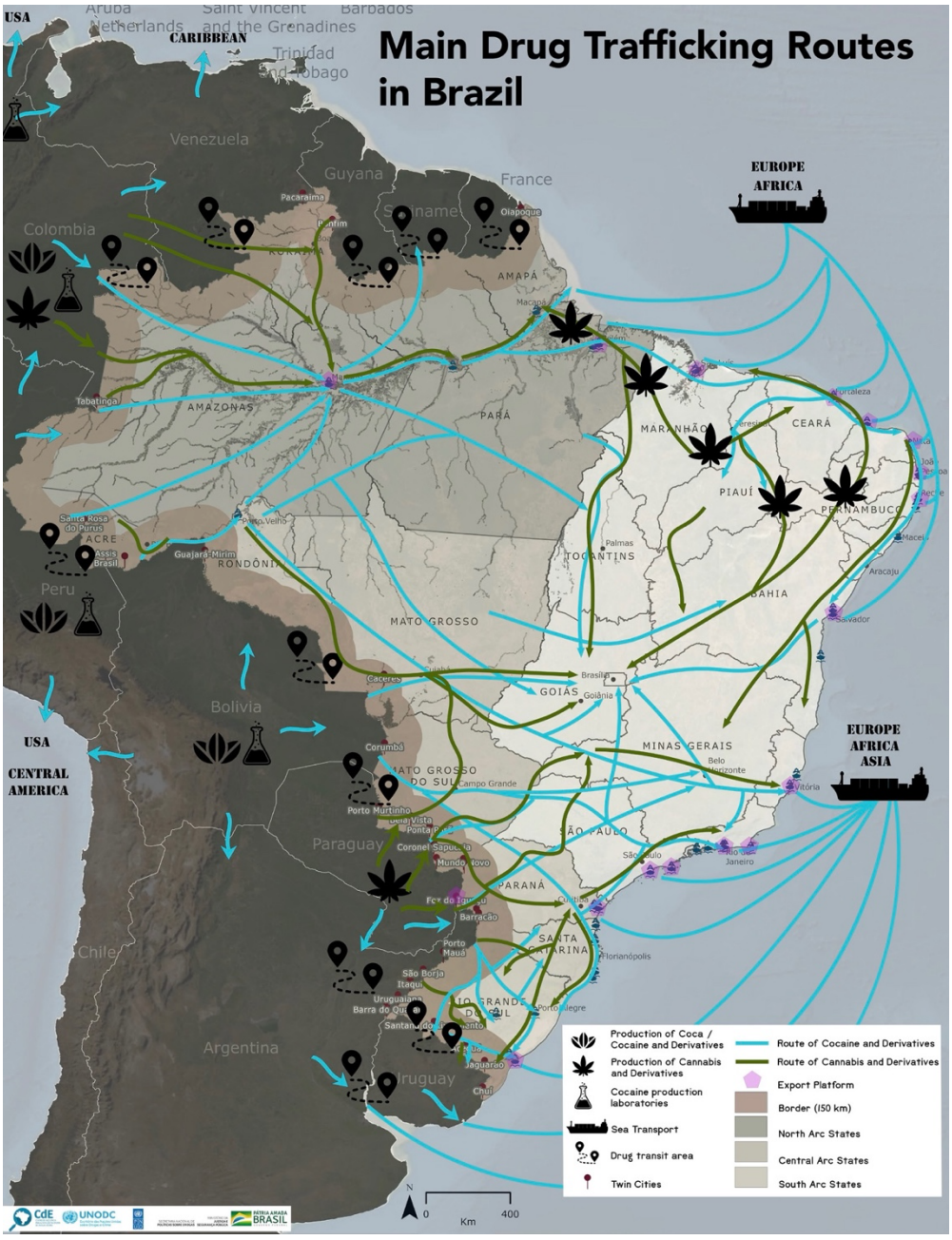


Figure 10: Main cocaine and marijuana trafficking routes in Brazil (COE Brazil, 2021).

Transnational criminal networks have been using Brazilian main exporting ports, especially the ports of Santos, Paranaguá, Salvador, and Itajaí, as "gateways" for cocaine shipment to reach its consumer markets overseas. The modus operandi of drug traffickers generally consists in hiding the drug inside containers through the rip-on/rip method, inside ships' compartments, and the "fishing" method. Criminals also create shell companies or impersonate a well-known company to disguise illegal business as legal. There is also corruption of port and ship operators to obtain information on port logistics and supply chain, or to escape surveillance and avoid control checks.

Most drug shipment that departs from Brazilian seaports is destined to European Ports, particularly the Port of Antwerp in Belgium and Algeciras in Spain (TCU, 2021). After Colombia, Brazil is the next major exporter of cocaine to the Belgium port, which is the main entrance gate of the drug in the European continent (UNODC, 2021). Recently, some smaller ports in Brazil are also being used as gateways to transport cocaine to Europe, as traffickers attempt to avoid the increased control and surveillance capacity of major ports.

The fact that Brazil is now a major transit country in international trafficking of cocaine is due to a transformation in the country's criminal landscape over the years. Brazil's largest and most well-known criminal groups, PCC ("*First Command of the Capital*") and CV (*Red Command*), originated respectively in São Paulo and Rio de Janeiro, have expanded its illicit activities, having taken a networked form by building connections with local factions in almost all Brazilian states. Besides, their criminal activities nowadays transcend national borders and include ties with transnational criminal organizations. With the elimination of intermediaries in the South America region, PCC and CV are now doing business directly with cocaine producers in Colombia, Bolivia, and Peru.

PCC is the largest criminal organization in Brazil, which functions as a decentralized criminal network operating in several clusters located mainly in São Paulo state and in other states of the country. PCC has lucrative business ties with drug cartels in landlocked Bolivia. The aim is to move Bolivian cocaine production across borders to reach the Atlantic Ocean. PCC has also criminal ties in Paraguay to attain logistic resources to transport cocaine cargo across the Brazilian border. Over the last years, PCC's illicit activities and criminal connections are increasingly gaining ground in Paraguay. The criminal organization controls several stages of cocaine trafficking logistics chain, from importation, transportation through the main transregional routes - in special the "Rota Caipira" (Hillbilly Route) that starts in Bolivia, goes

through Paraguay, and enter Brazilian territory leading to Port of Santos - to exportation to overseas markets, especially in Europe.

Recent arrests of "Ndrangheta" members, in 2019 and 2021, by Brazilian Federal Police working in cooperation with Interpol and the Carabinieri Police in Italy show that the Italian criminal group is in a lucrative tie-up with South American drug manufactures and PCC. In 2020, "Ndrangheta" members operating in Brazil orchestrated the purchased of large quantities of cocaine from PCC and South American drug cartels. The cocaine cargos were smuggled hidden inside containers of trade and cruise ships headed to European ports of Valencia (Spain), Gioia Tauro (Italy), and Rotterdam (Holland) (ADORNO, 2021).

2.5 Security Governance in Brazilian Seaports

Given the strategic importance of seaports for Brazil's economy and supply chain, and the complex criminality that takes place in its facilities, the provision of port security involves a myriad of municipal, state, and federal public actors and private actors as well. The scenario is very much alike the one described in part I of this chapter, where port security governance involves interagency arrangements, such as *ad hoc* joint task forces and operations, and also hybrid policing, across the local and global dimensions.

The security governance of the country's major seaports complies with the ISPS Code mandatory regime, in which terminals are responsible for developing risk assessments, Port Facility Security Plan, and designating PFSOs, which are accredited by CESPORTOS/CONPORTOS. The Port Authority Guard is responsible for the surveillance and security provision across the Organized Port (public area of ports), including access control to port area and facilities through identification of personnel, visitors, and vehicles. Besides, each terminal also hires their own private security teams, while the scanning of containers is usually carried out by hired third-party companies. Crime prevention and repression involves high and low policing and customs actors, such as the Federal Police, by way of NEPOM (The Maritime Federal Police), the Federal Revenue Office, and local civil and military police. Security is aided by advanced control and surveillance technologies, as well as integrated systems and databases.

In Brazil, there has been in recent years an overwhelming rise in cocaine apprehensions by law enforcement in the country's largest and most busy ports (see figure 11). In 2021, the Brazilian Federal Revenue Office seized more than 17 tons of cocaine in the Port of Santos during several operations throughout the year (BRASIL, 2021a). Most of the drugs seized are

headed to Europe, Africa, and Asia. Below, figure 12 shows the main destinations of cocaine trafficking departing from Brazilian ports.

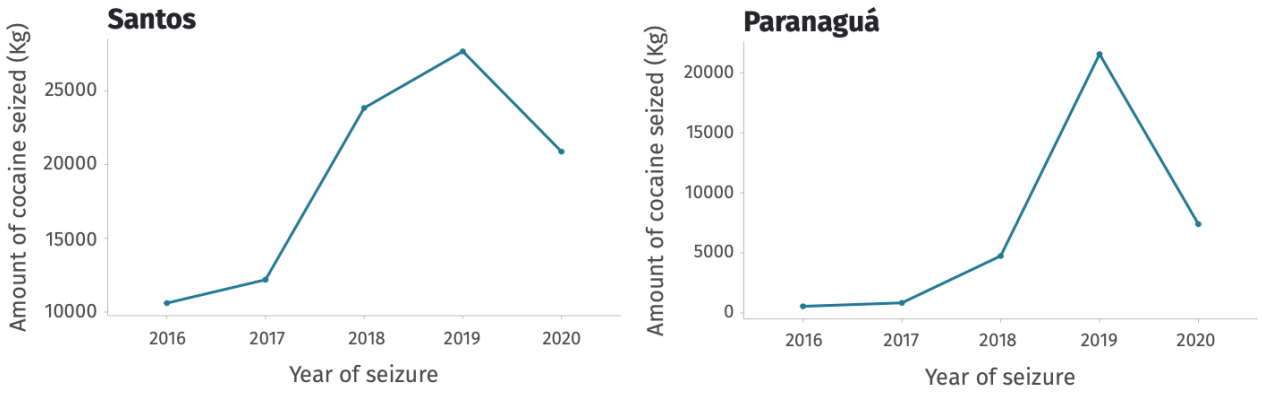


Figure 11: Cocaine seizures from 2016-2020 (COE Brazil, 2021).

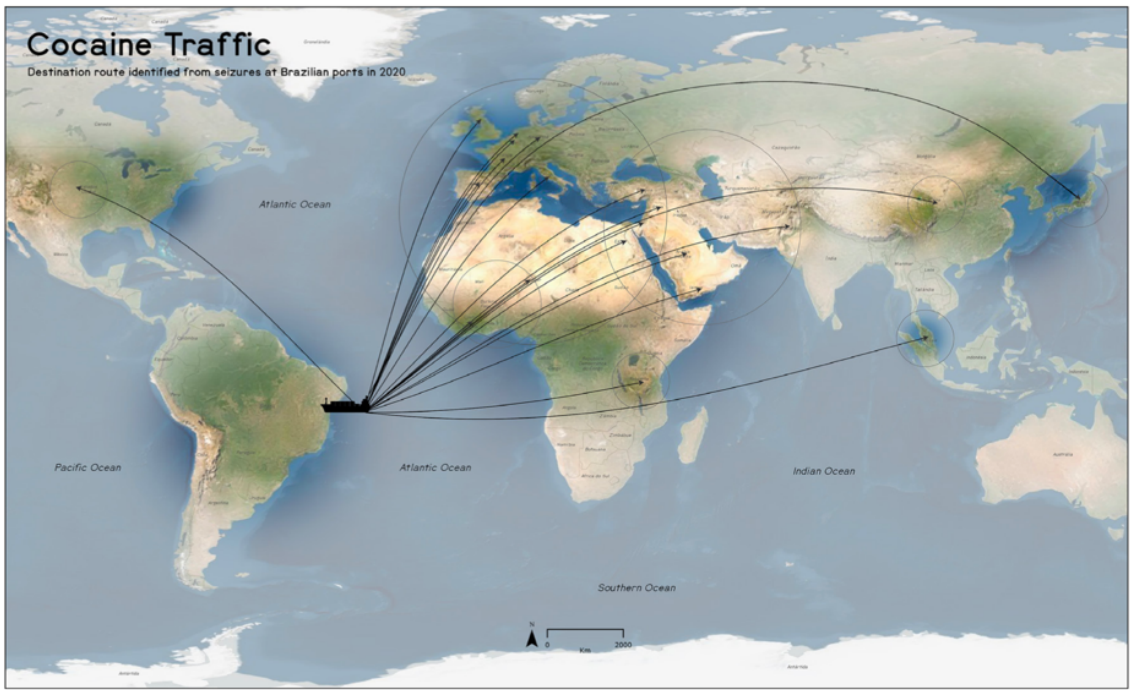


Figure 12: Cocaine trafficking routes departing from Brazil (COE Brazil, 2021).

Interagency Cooperation in Brazil

Interagency cooperation and joint task forces and operations are pivotal for the huge amounts of cocaine seized in the country by land, air and sea modes in recent years. Law enforcement integrated actions to prevent and repress cross-border crimes are carried out under programs such as VIGIA (The National Program for Border Security) and Blue VIGIA (under development to cover the maritime frontier), established by the Ministry of Justice and Public Security (MJSP), and PPIF (The Integrated Program for Border Protection), instituted by the Federal Government's GSI (The Institutional Security Office). The Ministry of Defense, by way of Joint Chiefs of Staff, also fosters the Joint Operation Ágata, which gathers the Brazilian Armed Forces, different Ministries, and several agencies to carry out tactical missions to repress cross-border crimes. Those programs and operations have shown to be very effective in controlling and repressing transnational crimes, by allowing the mobilization of resources, enhanced capacity, exchange of information, and data sharing through coordination and cooperation efforts among several agencies, police forces, and the Armed Forces, across the local and national levels.

In two seminars on maritime and port security, which took place recently in Brazil (I SEMINÁRIO INTERNACIONAL SOBRE TRÁFICO POR TRANSPORTE AQUAVIÁRIO, 2022; SEMINÁRIO DE APREENSÃO DE DROGAS NOS PORTOS, 2020), practitioners highlighted the crucial role that interagency cooperation and joint task forces and operations play in tackling criminality in ports. Most cocaine seizures and drug traffickers' arrests in ports and vessels usually happen under coordinated efforts between a number of security actors, such as NEPOM, the Brazilian Federal Revenue Office (RFB), the Brazilian Navy (MB), and other regulatory agencies, for instance. The cooperation with the Port Authority Guard and private security organizations is also important for the effectiveness of such operations in port facilities. In the case of the Port of Santos**,** since 2016, CESPORTOS-SP has stepped up the synergy among public and private security actors across the port, with training programs and simulations, in accordance with the ISPS Code. The results are seen in the record numbers of cocaine seizures in recent years.

Port Security in not without criticism in Brazil. A recent assessment by the Brazilian Federal Court of Accounts (TCU, 2021), commissioned to evaluate the work carried out by the Federal Police by way of NEPOM, CESPORTOS and CONPORTOS, and the provision of security in port facilities monitored by CESPORTOS, revealed a number of problems. The NEPOM units surveyed lacked personnel and the resources (such as patrol vessels) to carry out

their work efficiently. Some port facilities were found to not fully adhere to CONPORTOS security provisions (Risk assessments, Port Facility Security Plans, or PFSO), which sometimes were lacking, outdated, or developed by a non-accredited security company. Moreover, the port security system maintained by CONPORTOS have difficulty integrating the actions of port security providers. Finally, the work of the Federal Police in preventing and repressing illicit drug tracking is hindered by restrictions imposed by the Brazilian Federal Revenue Office regarding access to scan imagens of containers. The assessment highlighted to urge to reestablish the National Plan for Port Public Security as way to foster better cooperation among the myriad of security providers to mitigate some of security issues found.

In the two seminars, government and security providers also discussed the challenges and limitations of interagency coordination and cooperation in Brazil in relation to conflicting mandates and jurisdiction of agencies, duplication or dispersion of efforts, lack of resources and personnel to carry out operations, limiting budgets, and time-consuming planning. In addition, there is the reality of criminal networks that are very adaptable and resilient to law enforcement disruption by constantly changing their *modus operandi* and routes, while operating a highly profitable activity under market logic. In this context, and to achieve stronger interagency integration to tackle criminal networks, security practitioners argued for the need to create new policies, strategies, and joint commands.

In this scenario, we believe that interagency arrangements can benefit from flexibility and adaptability to rapid changing circumstances by adopting a network perspective on security. The concept of security network seems one optimal arrangement to achieve more sustainable and resilient cooperation and coordination among Brazilian agencies, when it comes to information sharing, knowledge generation, mobilization of resources, enhanced capacity, and so on. In this light, this report presents in the next section an illustrative model for a Knowledge-Generating Security Network designed to enhance the security governance of the Port of Santos.

2.6 A Knowledge-Generating Security Network for the Port of Santos

In this section, we propose a model for a Knowledge-Generating Security Network for the Port of Santos, based on the network properties and characteristics presented in the first chapter of this report. We point out that the security network model presented in this section is intended as an illustrative exercise to disseminate the network approach and the concept of Security Network among public security policy and decision makers and practitioners, as well as academia researching on ports. Designing a real operating network would require empirical

research on the security environment of the port to map the security actors and gather real data on agencies' relationships, capabilities, and resources, which is beyond the scope of this report.

Port security empirical research in Brazil is very scarce and to design the proposed security network, we used information from the Port of Santos website, government websites, and legislation regarding Brazilian port security to map the network actors and their legal attributions and jurisdictions. We also based the design of the network on information found in empirical research (PATRIARCA; LOPES, 2020) conducted on the security network of the Port of Santos. The research aimed to map the actors that compose the security network of the port to identify which ones occupy central positions in the network. For that, the authors made use of SNA tools, especially centrality measures, and carried out interviews with representatives of security agencies and content analysis in relation to which Capitals (Political, Social, Economic, Cultural, and Symbolic) contributed to actor's centrality in the network.

Regarding Social Capital, Patriarca and Lopes (2020)'s research found that CESPORTOS holds a relevant position in the security network of the Port of Santos. Its interagency collegiate structure allows the commission to connect with each one of its members agencies in the network. The formal and informal relations among the representatives enable the commission to mobilize the institutional resources of the agencies that constitute the collegiate, as well as the resources of their individual connections. Besides, its relationship with private actors allows the commission to disseminate relevant communications to all terminals in the port area (PATRIARCA; LOPES, 2020).

Given the significant Social Capital of CESPORTOS within the security arrangement of the Port of Santos, we suggest that the commission could occupy the position of a Lead Organization in a Knowledge-Generating Security Network for the port. Our suggestion is supported by one of the competencies of CESPORTOS, stated in Resolution No. 53, of September 4, 2020, which is to promote integration with other national and international security actors.

We point out, considering the methodological approach presented in this report, that due to CESPORTOS' interagency structure, the commission can be understood as a network in itself, with a narrow focus, as discussed in section 1.4.4 of this report, intended at carrying out auditing and inspections in the port's terminals. We acknowledge the existence of networks within networks, and CESPORTOS can be seen as a network within the proposed Knowledge-Generating Security Network. However, since our proposed network entails a wider scope, contemplating the myriad of internal and external security agencies and other organizations that have a stake in the delivery of port security, CESPORTOS is considered an organization within

the network structure, occupying the role of a catalytic actor. Our approach for the security network model aligns with the Inter-Organizational Network literature presented in the first chapter of this report, which states that in most goal-oriented security networks, an organization or agency that has a crucial role in the aim of the network is appointed to recruit the participants and articulate its objectives.

The Knowledge-Generating Security Network would operate similar to a PSKN, that is, as broader focus network contemplating internal and external security actors and stakeholders across jurisdictions and levels of government, which would function as communication channel to provide its actors access to other actors' knowledge in a timely manner according to specific needs. We point out that knowledge in security networks is understood as processed information enabling decision-making. In the security field, Knowledge-Generating networks are created, for example, for threat assessments in relation to organized crime and terrorism, and as evidence-based policing networks that seek to identify and disseminate best-practices.

In this light, the goals of the proposed security network would be to provide knowledge sharing on organized crime threat assessment, disseminate security best practices, and foster advanced learning, strengthening the synergy among public and private actors within the security governance of the Port of Santos. The main outcome of the proposed network would be to support a more substantiable and long-term interagency cooperation among the security providers of the port.

In the next sections, we discuss the relational structure and some managerial aspects of the proposed network and its potential outcomes. Our aim is to show the reader how the network characteristics and properties discussed in chapter one of this report can be applied to design and implement a model for a security network. We call attention to the illustrative nature of the network graph presented below, which was designed with no actual data on relational ties, and it did not employ any type of measure.

2.6.1 The Network Model - Relational Structure

The network design chosen for the proposed Knowledge-Generating Security Network is based on a "Lead Organization" type of governance (PROVAN and KENIS, 2008), in which a single organization acts as a highly centralized broker in charge of key decisions and all major network-level activities. CESPORTOS, as lead organization, could act as a centralized hub to gather information, facilitate communication, and disseminate knowledge among network actors. Below, we present the list of network actors with abbreviations, and the graph and matrix

representations of the model for the Knowledge-Generating Security Network (elaborated by the author), followed by a discussion on the proposed network relational structure.

List of Actors and Abbreviations (in the graph and matrix)

Core actors (blue circles):

CESPORTOS-SP - Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis [State Commissions for Public Security of Ports, Terminals, and Waterways]
PF – Policia Federal [Federal Police]
RFB – Receita Federal do Brasil [Federal Revenue Office]
CP-MB – Capitania dos Portos – Marinha do Brasil [Captain of the Port -Brazilian Navy]
ANTAQ – Agência Nacional de Transportes Aquaviários [National Waterway Transport Agency]
SPA – Santos Port Authority, represented by the Port Guard
SSP-SP – Secretaria de Segurança Pública do Estado de São Paulo [Public Security Office of São Paulo]
PSO – Private Security Organizations
TE – Terminals, represented by PFSOs
CONPORTOS - Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis [National Commission for Public Security of Ports, Terminals, and Waterways]

Peripheric Actors (blank circles):

RA – Regulatory Agencies
GSI/PPIF – Gabinete de Segurança Institucional/Programa de Proteção Integrado de Fronteiras [Institutional Security Office of the Federal Government/ The Integrated Program for Border Protection]
SEOIP – Secretaria de Operações Integradas - Ministério da Justiça e Segurança Pública [Integrated Operations Office - Ministry of Justice and Public Security]
ABIN - Agência Brasileira de Inteligência [Brazilian Intelligence Agency]
PRF – Polícia Rodoviária Federal [Federal Highway Police]
FA – Forças Armadas [Armed Forces]
IO – International Organizations
Other CESPORTOS

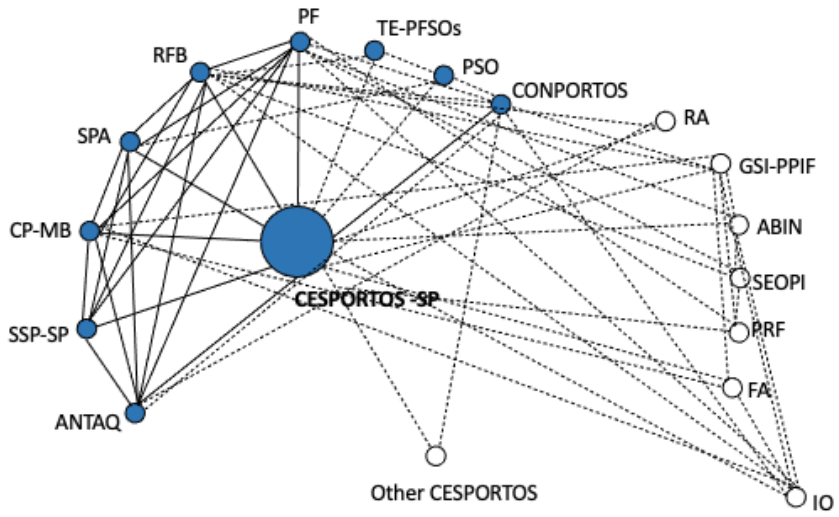


Figure 13: Knowledge-Generating Network Graph (Source: Author)

Table 17: Port of Santos Knowledge-Generation Network Matrix (Source: Author)

	CESPORTOS	PF	RFB	CP-MB	ANTAQ	SPA	SSP-SP	PSO	TE	CONPORTOS	GSI/PPIF	SEOIP	RA	FA	PRF	ABIN	IO
CESPORTOS	0	2	2	2	2	2	2	1	1	2	1	1	1	1	1	1	1
PF	2	0	2	2	2	2	2	1	1	0	1	1	0	0	1	1	1
RFB	2	2	0	2	2	2	2	1	1	1	1	1	1	1	0	1	1
CP-MB	2	2	2	0	2	2	2	0	1	0	0	0	0	0	0	0	1
ANTAQ	2	2	2	2	0	2	2	0	1	1	0	0	1	0	0	0	0
SPA	2	2	2	2	2	0	2	1	1	0	0	0	0	0	0	0	0
SSP-SP	2	2	2	2	2	2	0	1	1	0	0	0	0	0	0	0	0
PSO	1	1	1	0	0	1	1	0	1	0	0	0	0	0	0	0	0
TE	1	1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0
CONPORTOS	2	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1
GSI/PPIF	1	1	1	1	0	0	0	0	0	0	0	1	0	1	1	1	1
SEOIP	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0
RA	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
FA	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1
PRF	1	1	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0
ABIN	1	1	1	0	0	0	0	0	0	0	1	1	0	0	1	0	0
IO	1	1	1	0	0	0	0	0	0	1	1	0	0	1	0	1	0
Other CESPORTOS	1	0	0	0	0	0	0	0		1	0	0	0	0	0	0	0

The proposed network model is of a one mode, unidirectional, valued network. The actors in the network (network boundaries) were chosen by their role in the security provision of the Port of Santos, as well as their knowledge and expertise on organized crime threat assessment and prevention and repression best practices, including regulatory agencies that play a role in disrupting organized crime activities and assets, and international security organizations. The tie that connects actors in the network is cooperation, which enables the flow of information and knowledge, and facilitates communication. The distribution of ties in the network takes into account actors' connections in relation to their legal attributions and jurisdictions in the provision of security.

In the graph, the blue circles represent the core actors of the network, and the blank circles represent the peripheric actors. The core actors in the network are the agencies that work in the port environment to deliver security and CONPORTOS. The peripheric actors are the agencies with a supporting role in the provision of security, that is, actors that hold complementary capacity and expertise. The solid lines represent strong ties, and the doted lines represent weak ties in the network. In the Matrix, ties are represented by 0 (absence of tie), 1 (weak tie), and 2 (strong tie).

The network design considered, according to Inter-Organizational Network literature, the need for networks to combine flexibility with structure. Therefore, it entails a selective integration among actors, in which strong ties are located within the core, that is, among agencies that have a representative working at CESPORTOS, while peripheric actors in the network are connected by weak ties. The only core actors with weak ties are the Terminals, represented by the PFSO, and the Terminal's Private Security Organizations, since they do not have representatives at CESPORTOS, but play an important role in the delivery of security within the port's facilities. The core actors with strong ties form a cluster in a way that the representatives that work in CESPORTOS have each a close connection to their own agency, as well as close relations to other agencies' representatives in the collegiate body. The formal and informal relations among CESPORTOS member agencies' representatives create a closure network structure, which is a source of Social Capital for CESPORTOS. Therefore, according to Burt's (2004) argument on Closure and Structural Holes, CESPORTOS' Social Capital supports building trust and reciprocity among core actors, while it bridges actors otherwise disconnected across the structural holes of the network.

The network model configuration aligns with research on Security Networks that shows the need for a network to be stable at its core, while maintaining flexibility at its periphery. The network core should consist of agencies that are central to network goals, while flexibility in

the periphery is advantageous for agencies less connected and whose involvement is less crucial. In this way, new agencies can enter whenever needed in a timely manner bringing new information and knowledge to core members, while less involved agencies can leave. In the case of the proposed network model, the core actors are agencies that work within the port facilities and need to communicate and exchange information and knowledge frequently. Whereas the peripheric actors can take part in the network in an *ad hoc* basis at request, or whenever that is a need to exchange specific information, disseminate a particular knowledge or best practice or share capacity a certain actor has considerable expertise on. Therefore, the peripheric actors in the network model represent only examples of agencies/organizations that could take part in the network having the flexibility to enter and exit when occasion arises.

Finally, regarding the flow of resources within the proposed network, CESPORTOS occupies a broker position, or a boundary spanner, that is, an actor connected to all other actors in the network, through strong or weak ties, who is capable of steering the flow of information and knowledge within the structural holes of the network, as well as controlling the projects that bring actors from distant parts of the network. Moreover, its broker position allows it to reach in a timely way novel and important information and knowledge from peripheric parts of the network.

2.6.2 Network implementation and management: challenges and desired outcomes

We have seen in chapter one of this report that network implementation and management is a complex and challenging task, especially regarding the size of the network, the variety of its actors, and its purpose(s). An inter-organizational network with many actors that span jurisdictions, sectors and levels of government usually represents a challenge to its managers and leaders. Our proposed security network model has a wide scope, which on one hand provides greater depth and breadth of knowledge to share, but on the other, given the myriad of actors, it presents more risks, costs, and barriers to overcome. The type of security network proposed in this report, for instance, could be challenging to establish without attaining legal authority and proper legislation. However, as the cost, risks, and barriers increase so do the potential benefits and overall public value, as discussed in section 1.4.4 of this work (Dawes et al., 2009).

Regarding management, CESPORTOS, as the lead organization, could appoint a work group or steering committee among its representatives to coordinate the activities of the network, reach out to other actors' knowledge, expertise, and capacity, establish

communication channels, and develop knowledge products, such as threat assessments and best practices, as well as promote network learning by way of seminars, for example. The steering committee would also determine the goals and priorities for the network, build consensus, especially among core actors, manage actors' divergent goals and conflicting organizational cultures, and reach agreements on technical merits and possibilities. One way to navigate such challenges would be for the steering committee to appoint project leaders that would communicate to other actors in the network, especially peripheric ones, according to their knowledge expertise and capacity. Each project leader would focus on a specific need or activity of the network creating venues for new knowledge to be disseminated quicker within the network. Furthermore, it would be important that core actors of the network build and maintain strong relations based on trust reciprocity and a shared vision for the network to mitigate organizational barriers and prevent unforeseen issues that could derail the efforts. For other management tasks and challenges of Inter-Organizational networks, see section 1.3.2 of this report.

The proposed network outcomes could be manyfold. Knowledge-Generating networks are known to be more on-going in nature without a pre-defined time to begin and end. Therefore, the proposed network could work as a perennial asset, fostering enhanced and integrated knowledge on threat assessments and other port security related issues. It could also promote capacity building and continuous shared learning and dissemination of best practices related the national and international port security scenarios, as it holds connections with International Organizations. For example, as discussed earlier in this report, the transnational nature of routes used by drug traffickers require knowledge and information from several agencies with different jurisdictions to trace those routes to inform more efficient and effective law enforcement operations. Also, knowledge products developed by the network could support the creation of new policies and regulations, aid in decision making, as well as enhance coordination of joint operations.

The knowledge generated by the network could be shared, discretionarily, with other regional CESPORTOS, in order to create a more resilient port security system in Brazil. The knowledge generated could also help standardize all CESPORTOS collegiate bodies procedures, so that decision making would not vary from one region to another, given the continental dimension and cultural differences of Brazil. Especially nowadays with criminal networks using smaller ports with less surveillance and control capacity to traffic drugs.

Finally, CESPORTOS, as a lead organization, could foster the development of a shared network culture within its core members by harmonizing goal consensus and balancing different

organizational cultures, as well as managing conflicting mentalities, practices, or processes. This could help core network members to negotiate diverging interests and priorities in the delivery of security, and even avoid duplication of efforts. A shared culture helps build, together with trust and reciprocity, more dense and strong relations among network core actors. As the central actor in the network, harnessing the Social Capital of CESPORTOS could promote collective action resulting in more long term, sustainable, and resilient interagency cooperation among port security actors.

Conclusion

This report was developed with the aim to disseminate the "network perspective" among Brazilian public security decision makers and providers, as well as policy makers, especially working in the field of interagency, with a focus on port security governance. Interagency programs and arrangements seek to integrate security agencies in cooperating efforts, such as in information exchange and joint operations, for example. In this context, we intended to raise awareness on the concept of Security Network that could foster more sustainable and long-term interagency cooperation to tackle transnational criminality in multifaceted environments such as ports. The background for the discussions was TOC operating as criminal networks that are highly adaptable and resilient to law enforcement disruption. These "dark" networks use seaport facilities as "doors" and "gateways" for international drug trafficking and related crimes.

We also sought to engage Brazilian Security and Defense academia in the potentialities of applying the theoretical and methodological tools of SNA within Security Governance and Criminality studies. SNA is a well-known and vast methodology to map actors and analyze their social relations in almost all areas of human interactions. The Network Theories and the concept of Social Capital presented in chapter I illuminated how cooperation, based on trust and reciprocity, is achieved in socio-structures, and how Social Capital can be advantageous for actors that take part in Inter-Organizational networks, such as Security Networks, to yield more effective outcomes. The advantages of Security Networks include:

- Networks are more flexible and adaptable, and driven by expectations of trust and reciprocity, in the short and long terms, making them more efficient in eliciting cooperation, resources exchange and mobilization, capacity acquisition, and managing risks.

- Networks are a suitable choice to tackle complex, or “wicked” problems, that is, problems that cannot be addressed by one single organization and that require collective action (coordination and cooperation) between different organizations.

- Interactions and exchanges among security actors are guided by the capacity to poll resources to increase effectiveness and decrease vulnerability. Security networks gather participants and resources across different professional and jurisdictional fields and even national borders.

- Researchers of Security Networks argue that a detailed knowledge of interactions that occur in the network can better inform security programs and strategies and guide interventions at the operational level.

- Given the myriad of actors, both public and private, who play a role in the security provision in the port environment, security networks seem to be an optimal formation to pool resources, increase capacity in cooperative efforts, resulting in a more efficient and effective delivery of security.

In the context of Brazilian ports, drug trafficking is considered the main crime carried out in port facilities. Because of the transnational and complex nature of criminal organizations, port security authorities in Brazil acknowledge the need for more interagency synergy and cooperation to prevent and repress the activities of these criminal networks. In this light, this report proposed a model for a Knowledge-Generating Security Network for the Port of Santos. The contributions of the proposed network would be:

- The proposed network would provide knowledge sharing on organized crime threat assessment, disseminate security best practices, and foster advanced learning, strengthening the synergy among public and private security actors within the security governance of the Port of Santos.

- CESPORTOS, as lead organization, could act as a centralized hub to gather information and knowledge from network actors, in order to disseminate them across the network and port environment when needed.

- CESPORTOS, as lead organization, could be a channel for network agencies and other organizations to communicate through it, facilitating coordination and cooperation in joint task forces and operations, for example.

- As a Knowledge-Generating type of network, it could provide long term cooperation among security actors, fostering strong relations, based on trust and reciprocity, between core members to yield a more effective security provision in the port.

- Knowledge developed by the network could support the creation of new policies and regulations, aid in decision making, as well as enhance coordination of joint operations.

- The network would also be an important asset to standardize all reginal CESPORTOS collegiate bodies' procedures, helping to support a more resilient port system in the country.

We highlight the theoretical, methodological, and international scope of this report due to scarce empirical research on port security and security networks in the Brazilian context. We also call attention to the illustrative nature of the proposed Knowledge-Generating Security Network, given the lack of empirical data on the relations of security providers and other organizations in the Port of Santos. This owns to the COVID-19 restrictions, and our difficulty in finding and engaging security organization representatives (both public and private) willing to share their work experience and relations with other security providers. Research in the Defense and Security field is sometimes hampered by security organizations' confidentiality and privacy concerns and other individual issues, which was the case of this report.

For future work, conducting empirical research on the potentialities of the proposed Knowledge-Generating Security Network, given a more favorable scenario, would be a novel and stimulating proposition that could yield interesting results for port governance decision makers, security practitioners, and even for public security policy makers. Moreover, the complexity of port governance and the multifaceted nature of port spaces, which gathers a myriad of public and private actors, account for an interesting and challenging ground for scholars to carry out research applying the network perspective.

Additional future work could include other endeavors involving multi-agency cooperation in ports, such as "Green Ports", sustainable ports in relation to SDGs (UN 2030 Agenda), and "Smart Ports". Such endeavors make up a fertile ground to explore the intricacies

of networks aimed at collective action towards innovation and sustainable development in a highly interconnected space such as ports. Considering the port sustainability UN 2030 Agenda in Brazil, the network perspective could contribute to advancing the implementation of the SDGs in Brazilian ports. Ports concentrate a myriad of stakeholders, both internal and external, that play different roles and have distinct perceptions of sustainability. In this light, mapping actors with a stake in port sustainable development and their formal and informal relations could advance the implementation of the agenda by fostering networks of cooperation.

References

ADORNO, L. **Corleones em São Paulo**. UOL Notícias (online), 2021. Disponível em: https://noticias.uol.com.br/reportagens-especiais/chefes-da-mafia-italiana-nem-disfarcaram-identidade-para-viver-e-negociar-drogas-por-anos-no-brasil/. Acesso em: 20 set. 2021.

AGÊNCIA NACIONAL de TRANSPORTE AQUAVIÁRIOS (Brasil). **Setor portuário movimenta 1,2 bilhão de toneladas de cargas em 2021**. 2022. Disponível em: https://www.gov.br/antaq/pt-br/noticias/2022/setor-portuario-movimenta-1-2-bilhao-de-toneladas-de-cargas-em-2021/. Acesso em: 15 jun. 2022

AGRANOFF. R. Inside Collaborative Networks: Ten Lessons for Public Managers. **Public Administration Review**, v. 66, p. 56-65, 2006. Disponível em: https://www.jstor.org/stable/4096570. Acesso em: 03 mai. 2022.

ALBUQUERQUE, C.E.P.; ANDRADE, F. S. Análise de riscos com ênfase na segurança portuária: o processo de avaliação de riscos da CONPORTOS e o ISPS Code. **Revista Brasileira de Ciências Policiais**, v.10, n.1, p. 99-124, 2019. Disponível em: https://oasisbr.ibict.br/vufind/Record/ANP_15c4f3c4347663b6993ea7aecf6a0fe6. Acesso em: 07 dez. 2021.

ANSELL, C.; GASH, A. Collaborative Governance in Theory and Practice. **Journal of Public Administration Research and Theory**, v.18, n.4, p 543–571, 2008. Disponível em: https://academic.oup.com/jpart/article/18/4/543/1090370. Acesso em: 12 ago. 2022.

ANTONELLI, M. An exploration of organized crime in Italian Ports from an institutional perspective. Presence and Activities. **Trends in Organized Crime**, v. 24, p.152–170, 2020. Disponível em: https://link.springer.com/article/10.1007/s12117-020-09400-z. Acesso em: 25 abr. 2022.

ARQUILLA, J.; RONDEFELDT. **Networks and netwars: The future of terror, crime, and militancy**. RAND Corporation, 2001.

BARDACH, E. Networks, Hierarchies, and Hybrids. **International Public Management Journal**, v.20, n. 4, p. 560-585, 2017. Disponível em: https://gspp.berkeley.edu/assets/uploads/research/pdf/Networks_Hierarchies_and_Hybrids.pdf. Acesso em: 09 abr. 2022

BORGATTI, S. P.; HALGIN, D. S. On Network Theory. **Organization Science**, v.22, n.5, 2011. Disponível em: https://pubsonline.informs.org/doi/abs/10.1287/orsc.1100.0641?journalCode=orsc. Acesso em: 08 mar. 2021.

BORGATTI et al. Network measures of Social Capital. **Connections**, v.21, n.2, 1998. Disponível em: https://www.researchgate.net/publication/313513572_Network_measures_of_social_capital. Acesso em: 26 mai. 2021.

BRASIL. Polícia Federal. **Segurança Portuária**. 2022. Disponível em: https://www.gov.br/pf/pt-br/assuntos/seguranca-portuaria. Acesso em: 10 jan. 2022

BRASIL. Ministério da Justiça e Segurança Pública. **PF prende, em João Pessoa/PB, um dos principais fugitivos da Justiça Italiana**. 2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/05/pf-prende-em-joao-pessoa-pb-um-dos-principais-fugitivos-da-justica-italiana. Acesso em: 15 jul. 2021.

BRASIL. Resolução no 53, de 4 de setembro de 2020. **Dispõe acerca da consolidação e atualização das Resoluções da Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis, conforme normas do Código Internacional para a Proteção de Navios e Instalações Portuárias (Código ISPS, da sigla em inglês)**. Diário Oficial da União, Brasília, DF: Ministério da Justiça e Segurança Pública/Secretaria Nacional de Segurança Pública/Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis Disponível em: https://portal.in.gov.br/en/web/dou/-/resolucao-n-53-de-4-de-setembro-de-2020-276156332. Acesso em: 24 set. 2021

BRASIL. **Plano Nacional de Segurança Pública Portuária**. Brasília, DF: Ministério da Justiça. Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis – CONPORTOS, 2002. Disponível em: https://www.gov.br/pf/pt-br/assuntos/seguranca-portuaria/planonacionalPNSPPjustiapontogov.pdf. Acesso em: 15 nov. 2021

BRASIL. Receita Federal. **Receita Federal faz apreensão histórica de cocaína no Porto de Santos**. 2021a. Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2020/12/receita-federal-faz-apreensao-historica-de-cocaina-no-porto-de-santos. Acesso em: 04 fev. 2021.

BREWER, R. **Policing the Waterfront. The Social Structure of Collaborative Crime Control**. 2012. 305f. Tese (Doctor of Philosophy) – Australian National University, Australia, 2012.

BREWER, R. Controlling crime through networks. **Regulatory Theory**, Sidney: Australia National University Press, 2017. Disponível em: https://www.researchgate.net/publication/314246754_Controlling_crime_through_networks. Acesso em: 24 jan. 2022.

BRIGHT, D.A.; WHELAN, C. **Organized Crime and Law Enforcement: A Network Perspective**. London: Routledge, 2020.

BRIGHT, D.A.; MALM, A. Illicit Network Dynamics: The Formation and Evolution of a Drug Trafficking Network. **Journal of Quantitative Criminology**, v.35, p. 237-258, 2019. Disponível em: https://link.springer.com/article/10.1007/s10940-018-9379-8. Acesso em: 21 mai. 2021

BRUN, A; MCAULIFFE, E. Social Network Analysis as a Methodological Approach to Explore Health Systems: A Case Study Exploring Support among Senior Managers/Executives in a Hospital Network. **International Journal of Environment Research on Public Health**,

v.15, n.511, 2018. Disponível em: https://pubmed.ncbi.nlm.nih.gov/29534038/. Acesso em: 13 jun. 2021.

BUERGER, C; EDMUNDS, T. Blue Crime: Conceptualizing Transnational organized crime at sea. **Marine Policy**, v.119, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S0308597X20300270. Acesso em: 12 nov. 2020.

BURT, R. **Structural Holes: The Social Structure of Competition**. Harvard: Harvard University Press, 1995. Disponível em: https://www.jstor.org/stable/j.ctv1kz4h78#:~:text=The%20basic%20element%20in%20this,important%20advantages%20for%20the%20entrepreneur. Acesso em: 03 mai. 2021.

BURT, R. **Brokerage and Closure: An Introduction to Social Capital**. Oxford: Oxford University Press, 2004.

BURT, R. Structural Holes versus Network Closure as Social Capital. **Social Capital: Theory and Research**, 2001. Disponível em: https://www.researchgate.net/publication/51992854_Structural_Holes_versus_Network_Closure_as_Social_Capital_In_Social_Capital_Theory_and_Research. Acesso em: 07 abr. 2021.

CANTON, R. **Interagency Cooperation: how can it best enhance compliance with the law?** In: 162ND INTERNATIONAL SENIOR SEMINAR. United Nations Asia and Far East Institute, n. 99, 2016. Disponível em: https://www.unafei.or.jp/publications/pdf/RS_No99/No99_VE_Canton_2.pdf. Acesso em: 03 ago. 2022.

CENTRE OF EXCELLENCE FOR ILLICIT DRUG SUPPLY REDUCTION. **COVID-19 and drug trafficking in Brazil: the adaptation of organized crime and the actions of police forces during the pandemic**. Brasília: Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos do Ministério da Justiça e Segurança Pública, United Nations Office on Drugs and Crime, United Nations Development Program, 2021.

COLEMAN, J. Social Capital in the Creation of Human Capital. **American Journal of Sociology**, 1988. Disponível em: https://www.jstor.org/stable/2780243?seq=1. Acesso em: 27 abri. 2021.

CONNOLLY et al. The facilitators of Interagency working in the context of European public service reform. **Journal of the Academy of Social Sciences**, v. 15, n.5, p. 533-547, 2020. Disponível em https://www.tandfonline.com/doi/full/10.1080/21582041.2020.1824078. Acesso em 21 jun. 2022.

DAWES, et al. From a “Need to know” to a “Need to share”: tangled problems, information boundaries, and the building of public sector knowledge networks. **Public Administration Review**, v. 69, n.3 p. 392-402, 2009. Disponível em https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-6210.2009.01987_2.x. Acesso em 11 ago.2022.

DUPONT, B. Delivering security through networks: Surveying the relational landscape of security managers in an urban setting. **Crime, Law & Social Change**, v.45, p. 165-184, 2006.

ESKI, Y. **Policing, Port Security and Crime Control: An Ethnography of Port Securityscape**. London: Routledge, 2016.

GERSPACHER, N; DUPOND.B. The Nodal Structure of International Police Cooperation: An Exploration of Transnational Security Networks. **Global Governance** v.13, n. 3, p. 347-364, 2007.

GLOBAL INITIATIVE AGAINST TRANACIONAL ORGANIZED CRIME. **The global illicit economy: Trajectories of transnational organized crime**. GI-TOC, 2021. Disponível em: https://globalinitiative.net/analysis/global-organized-crime/. Acesso em: 10 jul. 2021.

GRANOVETTER, M. The Strength of Weak Ties. **American Journal of Sociology**, 1973. Disponível em: https://www.jstor.org/stable/2776392?seq=1. Acesso em: 15 fev. 2021.

HOLLEY and SHEARING. Chpater 10 A nodal perspective of governance: Advances in nodal governance thinking. **Regulatory Theory: Foundations and applications**, p. 163-180 2017. Disponível em: https://www.jstor.org/stable/j.ctt1q1crtm.18#metadata_info_tab_contents. Acesso em: 05 dez. 2021.

INTERNATIONAL MARITIME ORGANIZATION. **Code of practice on security in ports**. Tripartite Meeting of Experts on Security, Safety and Health in Ports, Geneva: IMO, 2003.

ISETT et al. Networks in Public Administration. **Journal for Public Administration Research and Theory**, v.21, p.157-173, 2011. Disponível em: https://www.jstor.org/stable/40961926. Acesso em 22 abr. 2021.

KNOKE, D.; YANG, S. **Social Network Analysis**. Nova York: SAGE Publications, 2020.

KRAHMANN, E. Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security. **Cambridge Review of International Affairs**, v. 18, n. 1, p.15-30, 2005.

LIN, N. A Network Theory of Social Capital. **Handbook on Social Capital**, 2005. Disponível em http://pro-classic.com/ethnicgv/SN/SC/paper-final-041605.pdf. Acesso em 25 fev. 2021.
MILWARD, H. AND PROVAN, K. A Manager's Guide to Choosing and Using Collaborative Networks. **Networks and Partnerships Series**, IBM Center for the Business of Government, 2006.

NOKLEBERG, M. The public-private divide revisited: questioning the middle ground of hybridity in policing. **Policing and Society**, v. 30, n.3, p.1-17, 2019. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/10439463.2019.1576673?journalCode=gpas20. Acesso em 13 fev. 2021.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Ocean Shipping and Ship Building**. OECD, 2019. Disponível em: https://www.oecd.org/ocean/topics/ocean-shipping/. Acesso em: 05 out. 2021.

PATRICARCA, G. and LOPES, C. A âncora da segurança portuária: como se caracteriza a rede organizacional de combate ao crime no Porto de Santos. In: ENCONTRO ANUAL DA ANPOCS, GT24: Mercados Ilícitos e Dinâmicas Criminais, 2020.

POPP et.al. Inter-Organizational Networks: A Review of literature to Inform Practice. **Collaborating Across Boundaries Series**, IBM Center for Business of Government, 2014. Disponível em: https://www.businessofgovernment.org/report/inter-organizational-networks-review-literature-inform-practice. Acesso em: 38 mar. 2022.

POMERLEAU, P. Public-Private Partnerships: Port Security. **Encyclopedia of Security and Emergency Management**, 2019. Disponível: https://link.springer.com/referenceworkentry/10.1007%2F978-3-319-69891-5_292-1. Acesso em 13 mai. 2022.

PRELL, C. **Social Network Analysis – history, theory & methodology**. London: SAGE Publications, 2012.

PROVAN, K; KENIS, P. Modes of Network Governance: Structure, Management, and Effectiveness. **Journal of Public Administration Research and Theory**, v.18, n.2, p. 229–252, 2008. Disponível em: https://www.semanticscholar.org/paper/Modes-of-Network-Governance%3A-Structure%2C-Management%2C-Provan-Kenis/58d8e2207074b6d5bcedcdfaa01b42270c301542.
Acesso em: 26 fev. 2021.

PROVAN, K; SYDOW, J. Interorganizational Networks at the Network Level: A Review of the Empirical Literature on Whole Networks. **Journal of Management**, 2007. Disponível em: https://journals.sagepub.com/doi/10.1177/0149206307302554. Acesso em: 06 nov. 2020.

PROVAN, K; LEMAIRE, R. Core concepts and Key Ideas for Understanding Public Sector Organizational Networks: Using Research to Inform Scholarship and Practice. **Public Administration Review**, 2012. Disponível em https://www.researchgate.net/publication/262085643_Core_Concepts_and_Key_Ideas_for_Understanding_Public_Sector_Organizational_Networks_Using_Research_to_Inform_Scholarship_and_Practice. Acesso em 27 abri. 2022.

PROVAN, K and SYDOW, J. Interorganizational Networks at the Network Level: A Review of the Empirical Literature on Whole Networks. **Journal of Management**, 2007. Disponível em https://journals.sagepub.com/doi/10.1177/0149206307302554. Acesso em 23 jan. 2022.

PUTMAN, R. The Prosperous Community – Social Capital and Public Life. **The American Prospect**, 1993. Disponível em: https://faculty.washington.edu/matsueda/courses/590/Readings/Putham%201993%20Am%20Prospect.pdf. Acesso em: 15 mai. 2021.
RAAB, J; MILWARD, H.B. Dark networks as problems. J**ournal of Public Administration Research Theory**, v.13, n.4, p. 413-439, 2003.

ROKS, R.; BISSCHOP, L; STARING, R. Getting a foot in the door. Spaces of cocaine trafficking in the Port of Rotterdam. **Trends in Organized Crime**, v.24. p 171–188, 2020. Disponível em: https://www.researchgate.net/publication/346132754_Getting_a_foot_in_the_door_Spaces_of_cocaine_trafficking_in_the_Port_of_Rotterdam. Acesso em: 03 abr. 2021.

SANTOS PORT AUTHORITY. **Fatos e Dados 2022**. SPA, 2022. Disponível em: https://www.portodesantos.com.br/wp-content/uploads/Facts-Figures-2022.pdf. Acesso em: 12 abr. 2022

I SEMINÁRIO DE APREENSÃO DE DROGAS NOS PORTOS, Brasília, DF: Gabinete de Segurança Institucional – Governo Federal, 2020.

SEMINÁRIO DE APREENSÃO DE DROGAS NOS PORTOS, Brasília, DF: Gabinete de Segurança Institucional – Governo Federal, 2020.

SERGI, A. **The Port-Crime Interface: A Report on Organized Crime & Corruption in Seaports**. Essex: University of Essex, 2020a.

SERGI, A. Policing the port, watching the city. Manifestations of organized crime in the port of Genoa. **Policing and Society**, v.31, p. 639-655, 2020b. Disponível em: https://www.semanticscholar.org/paper/Policing-the-port%2C-watching-the-city.-of-organised-Sergi/8906109557c314138c2f6423e864ac2548f8f9a0.
Acesso em: 15 de abr. 2021.

SERGI et al. **Ports, Crime and Security. Governing and Policing Seaports in a Changing World**. Bristol: Bristol University Press, 2021.

SERGI, A. Playing Pac-Man in Portville: Policing the dilution and fragmentation of drug importations through major seaports. **European Journal of Criminology**, 2020c. Disponível em: https://journals.sagepub.com/doi/full/10.1177/1477370820913465. Acesso em 13 set. 2021.

SIMPLILEARN. Social Network Analysis. Online course, 2022. Disponível em https://www.simplilearn.com/. Acesso em 04 abr. 2022.

STABER, U. Social Capital or Strong Culture? **Perspectives on Research**, v.5, p. 413-420, 2003. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/13678860210154422?journalCode=rhrd20. Acesso em: 15 abr. 2021.

STRICKLER, T. Interagency Cooperation: Quo Vadis? **Interagency Journal**, v.1, n.3, 2010. Disponível em: http://thesimonscenter.org/wp-content/uploads/2010/11/IAJ-1-1Fall2010.pdf. Acesso em: 03 mar. 2022

TRIBUNAL DE CONTAS DA UNIÃO (Brasil). **Relatório de Auditoria – Segurança Pública nos Portos, Terminais e Vias Navegáveis**. Brasília, DF: TCU: 2021. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-constata-que-policia-federal-portuaria-esta-com-regulamentacao-defasada-e-descumpre-normas-de-seguranca.htm. Acesso em: 02 jul. 2021.

UNITED NATIONS. Resolution 55/25 of 15 November 2000. **The UN Convention against Transnational Organized Crime.** UN General Assembly**,** 2000**.** Disponível em: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf.
Acesso em: 3 de mar. 2021.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **The World Drug Report 2021.** United Nations, 2021. Disponível em: https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html. Acesso em: 10 jun. 2021.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **The World Drug Report 2022.** United Nations, 2022. Disponível em https://www.unodc.org/res/wdr2022/MS/WDR22_Booklet_4.pdf. Acesso em 05 jun. 2022.

WASSERMAN, S.; FAUST. K. **Social Network Analysis – Methods and Applications**. Cambridge: Cambridge University Press, 2009.

WHELAN, C.; DUPONT, B. Taking stock of networks across the security field: a review, typology and research agenda. **Policing and Society**, v.17, p 671-687, 2017. Disponível em https://www.researchgate.net/publication/318731217_Taking_stock_of_networks_across_the_security_field_A_review_typology_and_research_agenda. Acesso em 23 nov. 2021.

WHELAN, C. Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration. **Security Journal**, v.30, p. 310-327, 2017. Disponível em:
https://www.researchgate.net/publication/270852976_Managing_dynamic_security_networks_Towards_the_strategic_managing_of_cooperation_coordination_and_collaboration
Acesso em: 01 jun. de 2021.

WHELAN, C. Organizational culture and cultural change: A network perspective**. Australian & New Zealand Journal of Criminology**, 2016. Disponível em https://journals.sagepub.com/doi/abs/10.1177/0004865815604196?journalCode=anja. Acesso em 23 nov. 2021.

WHELAN, C. **Networks and National Security: Dynamics, Effectiveness and Organization**. London: Routledge, 2012.

YANG, S.; KELLER, F. B.; ZHENG. Chapter I Basics of Social Network Analysis. **Social Network Analysis: Methods and Examples**, 2017.